Satakunnan ammattikorkeakoulu
Satakunta University of Applied Sciences

KARI SALONEN

Esineiden internet

Älykodit

TIETOJENKÄSITTELYN KOULUTUSOHJELMA
2021

Tekijä(t) Salonen, Kari	Julkaisun laji Opinnäytetyö, AMK	Päivämäärä syyskuu 2021
	Sivumäärä 26	Julkaisun kieli Suomi
Julkaisun nimi **Esineiden internet – Älykodit**		
Tutkinto-ohjelma Tietojenkäsittelyn koulutusohjelma		
Opinnäytetyön aiheena on IoT eli esineiden internet. Siinä käsitellään internettiin liitettävien esineiden ja asioiden hyödyntämistä eri ympäristöissä, niin kuluttajan arjessa, kotona kuin laajemmin meitä ympäröivässä yhteiskunnassa. Tämän opinnäytetyön tarkoituksena on selventää yleisellä tasolla, mitä on esineiden internet ja mitä se tarkoittaa kotitalouksille. Työssä tarkastellaan mitä esineiden internet tuo mukanaan sen yleistymisen myötä ja mitä se merkitsee. Sen jälkeen työssä selvitetään mitä se tuo tullessaan kotitalouksille ja rakennuksille ja miten sitä voi soveltaa käytännössä. Lopuksi vielä tarkastellaan esineiden internetin tuomia tietoturvan ja yksityisyyden ongelmia.		
Asiasanat Esineiden internet, IoT, Älykodit		

Author(s)	Type of Publication	Date
Salonen, Kari	Bachelor's thesis	September 2021
	Number of pages 26	Language of publication: Finnish

Title of publication
Internet of Things – Smart homes

Degree program
Business Information Systems

The subject of the thesis is IoT or the Internet of Things. The thesis describes how to utilize objects and things that are connected to the internet in different environments which can be homes and in everyday life or in the society surrounding us.

The purpose of the thesis is to clarify what is IoT in general and what it means to households. The thesis contains information about IoT and what happens when it becomes more common and also what this might mean to society. The thesis also contains information about households and buildings; how IoT affects them and how to benefit from its qualities. In the end of the thesis, there's a chapter about the security and privacy issues that IoT manifests.

Key words
Internet of Things, IoT, Smart homes

SISÄLLYS

1 JOHDANTO

Internet of Things (IoT) tai esineiden internet on kovaa vauhtia kasvava tietotekniikan ala, varsinkin nyt kun 5G mobiiliverkot ovat yleistymässä ympäri maailma. Markkinoille on tulossa koko ajan lisää tuotteita ja ohjelmistoja, jotka ovat keskenään yhdistettynä internetin kautta. Esineiden internet tuo paljon mahdollisuuksia monelle alalle, niin teollisuudelle kuin kotitalouksille.

Opinnäytetyöni alussa tarkastelen yleisesti, mitä tarkoitetaan termillä IoT eli esineiden internet. Annan esimerkkejä tietojen keräämisestä, niiden vastaanottamisesta ja siitä, miten tietoja käsitellään ja miten niiden perusteella toimitaan. Omien henkilökohtaisten mielenkiinnon kohteideni ja vahvuuksieni pohjalta annan esimerkkejä siitä, miten kuluttaja pystyy internettiin liitettyjä esineitä ja asioita hyödyntämään omassa arjessa, työpaikallaan tai lähipiirissään. Tarkastelen myös erilaisia yhteystyyppejä, koska tavat, joilla esineet voidaan yhdistää toisiinsa tai internettiin on olennainen osa esineiden internettiä.

Olen tietojenkäsittelyn opintojeni ulkopuolella tutustunut laajemmin myös tietoturvaan koskevaan kirjallisuuteen, joten pidin tärkeänä sisällyttää opinnäytetyöhöni hyötyjen lisäksi, myös internetin ja tietojen analysoinnin mukanaan tuomat riskit. Esineiden internet tuo mukanaan haasteita myös valmistajille. Mitä kaikkea sille kerätylle datalle, jota esineiden internet tuottaa, tulee tehdä ja mihin dataa säilötään? Se tuo mukanaan myös huolia ihmisten yksityisyydensuojalle ja tietoturvalle. Monesti ongelmana on yhteisten standardien puute.

Esineiden internet on yleistymässä niin kodeissa kuin vapaa-ajalla, ja internettiin liitettyjä esineitä löytyy sekä lapsille, vanhemmille kuin ikäihmisillekin. Ne tarjoavat ihmisille helpompia tapoja hallita elämäänsä, luovat turvallisuutta ympärilleen ja kehittävät yhteyskuntaa ympäristöystävällisemmäksi ja taloudellisemmaksi luoden parempaa tulevaisuutta.

2 MITÄ ON ESINEIDEN INTERNET

Internet of Things (IoT) on suomennettuna asioiden tai esineiden internet. Se tarkoittaa muun muassa esineitä, laitteita ja antureita, jotka ovat kytkettynä internettiin ja pystyvät lähettämään ja vastaanottamaan tietoa. Laajimmassa merkityksessä termi IoT kattaa kaiken, mikä on yhteydessä Internetiin, mutta sitä käytetään yhä enemmän määrittelemään esineitä, jotka "puhuvat" keskenään (Burges 2018). Tiedonkerääminen ja sen jakaminen on olennainen osa IoT:ta. Kun kerättyä tietoa jaetaan muiden laitteiden tai käyttäjien kesken, pystytään toimimaan sen mukaan. Toiminto mitä saadun datan mukaan tehdään voi olla joko automaattista tai käyttäjän itse määrittelemää.

IoT-ekosysteemi koostuu verkkoa käyttävistä älylaitteista kuten prosessoreista, antureista ja tietoliikennelaitteistoista, jotka käyttävät sulautettuja järjestelmiä keräämällä, lähettämällä ja toimimalla niiden ympäristöstä saadulla datalla. IoT-laitteet jakavat keräämänsä anturitiedot yhdistämällä IoT-yhdyskäytävään tai muuhun reunalaitteeseen, jossa tiedot analysoidaan pilvessä tai paikallisesti. Joskus nämä laitteet kommunikoivat muiden niihin liittyvien laitteiden kanssa ja toimivat niiltä saatujen tietojen mukaan. (Gillis 2020.) Laitteet tekevät suurimman osan työstä ilman ihmisen väliintuloa, vaikka ihmiset voivat olla vuorovaikutuksessa laitteiden kanssa, esimerkiksi asentaa ne, antaa niille ohjeita tai käyttää niiltä saatuja tietoja.

IoT:n yksi keskeisimmistä osista on siellä olevien esineiden tunnistustarve käyttäjiä kohtaan. Tunnistusta voidaan tehdä monin eri tavoin. Käyttäjän tunnistus tarkoittaa käyttäjän profiilia ja siihen liitettävää dataa, joka tulee monista eri lähteistä. Käyttäjädataa keräävät profiiliin esimerkiksi älypuhelimet, internetsivustot, esineet ja vaikkapa kaupassa liikkuminen, missä kasvojentunnistusohjelmalla asiakas voidaan liittää hänen käyttäjäprofiiliinsa. Käytännössä IoT:ssa olevat esineet voivat tunnistaa käyttäjänsä useilla eri tavoilla, kuten sormenjäljillä, kasvojentunnistuksella, käyttäjätunnuksella tai vaikkapa henkilökohtaisella varmenteella, joka voi olla kännykässä. IoT:ssa ei ole oleellista kuka seuraa, vaan se mikä seuraa käyttäjää. (Ryynänen 2016.)

Ryynäsen (2016) mukaan on odotettavissa, että IoT tulee tekemään useille eri kulutustavaroille muutoksen. Tämä on verrattavissa siihen, mikä on tapahtunut tuotteille,

joiden fyysinen olomuoto ja kulutustottumukset ovat muuttuneet internetin kehittymisen myötä. Siinähän esimerkiksi CD-levyt ovat muuttuneet musiikkipalveluiden kautta ladattavaksi musiikki tiedostoiksi, jonka jälkeen ovat tulleet musiikin suoratoistopalvelut. Toisin sanoen, ennen kaupasta ostettu fyysinen levy muuttui palveluksi, jonka jakelua hallitsee palveluntarjoaja. Kuluttaja ei siis omista enää fyysistä kopiota, vaan kuluttuja käyttää palvelua jonkinasteista korvausta vastaan.

Toisenlaisena esimerkkinä, melkein mikä tahansa fyysinen esine voidaan muuntaa IoT-laitteeksi, jos se voidaan yhdistää Internetiin ohjattavaksi tai tiedon välittämiseksi (Ranger 2020; Meola 2021). Hehkulamppu, joka voidaan kytkeä päälle älypuhelinsovelluksella, on IoT-laite, samoin kuin liiketunnistin tai älykäs termostaatti toimistossa tai keskukseen liitetty katuvalo. IoT-laite voi olla yhtä pörröinen kuin lapsen lelu, tai yhtä vakava kuin kuljettajaton kuorma-auto. Se voi olla ranteessa pidettävä kello, tai auto, jonka voi kutsua tulemaan sinun luoksesi. Jotkut suuremmat kohteet voivat itse olla täynnä monia pienempiä IoT-komponentteja, kuten suihkumoottori, joka on nyt täynnä tuhansia antureita, jotka keräävät ja lähettävät tietoja takaisin varmistaakseen, että se toimii tehokkaasti. Vielä suuremmassa mittakaavassa ”älykkäät kaupungit” -hankkeet täyttävät kokonaisia alueita antureilla, jotka auttavat meitä ymmärtämään ja hallitsemaan ympäristöä.

2.1 Tietojen käsittely

Kun jokin esine tai asia on kytkettynä internetiin, se tarkoittaa, että se voi lähettää tai vastaanottaa tietoja tai jopa molempia. Kyky lähettää ja vastaanottaa tietoja tekee asioista älykkäitä. Esimerkiksi älypuhelimella voi kuunnella mitä tahansa kappaletta maailmassa, mutta se ei tarkoita, että jokainen maailman kappale olisi tallennettuna puhelimeen, vaan se johtuu siitä, että jokainen maailman kappale on tallennettu jonnekin muualle ja puhelimesi voi kysyä jotain kappaletta ja sen jälkeen vastaanottaa tietoa eli suoratoistaa kyseistä kappaletta. Asioiden internetissä asiat, jotka ovat yhteydessä internetiin voidaan jakaa kolmeen luokkaan:

- asiat, jotka keräävät ja lähettävät tietoa
- asiat, jotka vastaanottavat tietoja ja toimivat sen jälkeen
- asiat, jotka tekevät molemmat.

Ja kaikilla näillä kolmella on valtavia etuja, jotka ruokkivat toisiaan. (McClelland 2020.)

2.1.1 Tietojen kerääminen ja lähettäminen

Joka päivä meitä ympäröivät anturit, jotka havaitsevat, mittaavat ja lähettävät tietoja jossakin muodossa. Anturit voivat olla lämpötila-antureita, liiketunnistimia, kosteusantureita, ilmanlaatuantureita tai valoantureita. Näiden lisäksi on antureita myös IoT-kuluttajalaitteista, kuten turvajärjestelmistä, älylaitteista, älytelevisioista ja puettavista terveysmittareista. Tiedot kerätään myös kaupallisista laitteista, mukaan lukien kaupalliset turvajärjestelmät, liikenteen seurantalaitteet ja sään seurantajärjestelmät. Nämä anturit toimivat reaaliajassa ja yhdessä internetyhteyden kanssa ne antavat meille mahdollisuuden kerätä automaattisesti tietoja ympäristöstä, mikä puolestaan antaa meille mahdollisuuden tehdä älykkäämpiä päätöksiä energian ja rahan säästämiseksi. (Shoemaker. 2019; McClelland 2020.)

Esimerkiksi maatilalla automaattisen tiedon saaminen maaperän kosteudesta voi kertoa viljelijöille tarkalleen, milloin heidän satonsa on kasteltava sen sijaan, että niitä kasteltaisiin liikaa, mikä voi tulla liian kalliiksi, tai liian vähän, mikä voi johtaa sadon menetykseen. Näin viljelijä voi varmistaa, että sato saa oikean määrän vettä. Aivan kuten näkökykymme, kuulomme, hajuaistimme, kosketusaistimme ja makuaistimme antavat meille ihmisille mahdollisuuden tuntea maailma ympärillämme, anturit antavat koneille mahdollisuuden tuntea maailman. (McClelland 2020.)

2.1.2 Tietojen vastaanottaminen ja toimiminen niiden perusteella

Valtava valikoima laitteita muodostaa yhteyden Internetiin ja jakaa tietoja anturien kautta päivittäin. Nämä tiedot ovat arvottomia ilman analyysiä. IoT-analyysiratkaisun avulla organisaatioiden tuottama data kerätään, analysoidaan ja tallennetaan tehokkaasti. Tämän seurauksena organisaatiot voivat optimoida toimintansa kaikilla tasoilla, parantaa päätöksentekoa ja saavuttaa useita etuja. (Khvoynitskaya 2019.)

IoT-antureiden ja data-analytiikan yhdistelmä voi auttaa yrityksiä etenkin teollisuudessa määrittämään, milloin laite vaatii huoltoa mittaamalla tärinää, lämpöä ja muita tärkeitä lukuja. Älylaitteet voivat myös lähettää käyttäjille viestejä mahdollisista vioista, kulumisesta ja toimitus ajoista. Tämä paitsi helpottaa laitteiden säännöllistä huoltoa, myös edistää ennakoivaa huoltoa. Anturitietoja käytetään ennustamaan, milloin laitteet on huollettava, mikä mahdollistaa huollon ajoituksen optimaalisella hetkellä, mikä vähentää rikkoontumisia ja säästää ylläpitokustannuksia. (Khvoynitskaya 2019.)

2.1.3 Tietojen kerääminen, lähettäminen ja vastaanottaminen yhdessä

Kuten kappaleessa 2.1.1 mainitussa esimerkissä. Anturit voivat kerätä tietoa muun muassa maaperän kosteudesta ja kertoa viljelijälle, kuinka paljon kastella satoa, mutta siihen ei tarvitse itse viljelijää. Sen sijaan kastelujärjestelmä voi käynnistyä automaattisesti tarpeen mukaan perustuen siihen, kuinka paljon kosteutta on maaperässä. Toisaalta jos kastelujärjestelmä saa tietoa tulevasta säästä internetin kautta ja näkee, koska sade alkaa, se voi päättää olla kastelematta satoa, koska sade kastelee ne joka tapauksessa. Kaikki nämä tiedot maaperän kosteudesta ja siitä, kuinka paljon kastelujärjestelmä kastelee satoa ja kuinka hyvin sato kasvaa, voidaan kerätä ja lähettää supertietokoneille, jotka suorittavat uskomattomia algoritmeja hyödyntääkseen näitä saamiaan tietoja. (McClelland 2020.)

2.2 Hyötyjä kuluttajalle

IoT lupaa tehdä kodeistamme, toimistoistamme ja ajoneuvoistamme älykkäämpiä ja mitattavampia. Älykkäät kaiuttimet, kuten Amazonin Echo ja Google Home, helpottavat musiikin toistamista, ajastinten asettamista tai tietojen saamista. Kodinturvajärjestelmien avulla on helpompaa seurata, mitä kodin sisällä ja ulkona tapahtuu. Sillä välin älykkäät termostaatit voivat auttaa meitä lämmittämään kotiamme ennen paluuta, ja älykkäät lamput voivat näyttää siltä, että olemme kotona, vaikka olisimme ulkona. Kodin ulkopuolella anturit voivat auttaa meitä ymmärtämään, kuinka meluisa tai saastunut ympäristömme voi olla. Itse ajavat autot ja älykkäät kaupungit voivat muuttaa tapaa, jolla rakennamme ja hoidamme julkisia tilojamme. (Ranger 2020.)

Kuluttajille älykoti on todennäköisesti paikka, jossa he todennäköisesti joutuvat kosketuksiin Internet-yhteensopivien asioiden kanssa, ja se on yksi alue, jolla suuret teknologiayritykset, kuten erityisesti Amazon, Google ja Apple kilpailevat kovasti. Näistä ilmeisimpiä ovat älykkäät kaiuttimet, kuten Amazonin Echo, Google Home tai Apple Homepod, mutta on myös älykkäitä pistokkeita, hehkulamppuja, kameroita, ovikelloja, termostaatteja, siivousrobotteja, rannekelloja, kahvinkeittimiä, pesukoneita ja jääkaappeja. (Ranger 2020.)

Älykkäitä laitteita kotona voidaan käyttää moneen tarkoitukseen. Ne auttavat jokapäiväisissä kodin askareissa, kuten pyykinpesussa ja siivouksessa, ne auttavat myös rentoutumaan ja kuluttamaan viihdettä, mutta niillä on myös vakavampi puoli. Ne voivat auttaa pitämään ikääntyneet itsenäisinä ja asumaan omissa kodeissaan ylläpitämällä kommunikointia perheen ja hoitajien kesken sekä seuraamalla heidän jokapäiväistä terveyttään. Parempi käsitys kotiemme toiminnasta ja kyky säätää näitä asetuksia, voisi auttaa säästämään energiaa esimerkiksi vähentämällä lämmityskustannuksia.

3 ÄLYKODIT

Älykoti on asuinpaikka, jossa pystytään hallinnoimaan laitteita etäältä, kuten valaistusta ja lämmitystä. Älykotitekniikka, jota usein kutsutaan myös kodin automaatioksi tai domotiikaksi (latinaksi "domus" tarkoittaa kotia), tarjoaa kodin omistajille turvallisuuden, mukavuuden, ja energiatehokkuuden antamalla heille mahdollisuuden hallita älylaitteita, usein matkapuhelimessa olevalla sovelluksella tai muulla verkkoon liitetyllä laitteella. Osa IoT:n älykkäistä kodin järjestelmistä ja laitteista toimii usein yhdessä jakamalla kuluttajien käyttötietoja keskenään ja automatisoimalla talon omistajien mieltymyksiin perustuvia toimia. (Chen 2020; Shea 2020.)

Älykkään kodin laitteet ovat yhteydessä toisiinsa, ja niihin pääsee käsiksi yhdestä keskipisteestä, kuten älypuhelimesta, taulutietokoneesta, kannettavasta tietokoneesta

tai pelikonsolista. Ovilukkoja, televisioita, termostaatteja, kodin näyttöjä, kameroita, valoja ja jopa laitteita, kuten jääkaappia, voidaan ohjata yhden kodin automaatiojärjestelmän kautta. Järjestelmä on asennettu mobiililaitteeseen tai muuhun verkkoon kytkettyyn laitteeseen, ja käyttäjä voi luoda aikataulut tiettyjen muutosten voimaantulolle. (Chen 2020.)

Älykkäissä kodinkoneissa on itseoppimistaitoja, jotta ne voivat oppia asunnon omistajan aikataulut ja tehdä muutoksia tarvittaessa. Älykkäät asunnot, joissa on valaistuksen tai lämmityksen säätö, antavat kodin omistajille mahdollisuuden vähentää sähkön käyttöä ja säästää energiakustannuksista. Jotkut kodin automaatiojärjestelmät varoittavat asunnon omistajaa, jos kotona havaitaan liikettä heidän poissa ollessaan, kun taas toiset voivat soittaa viranomaisille kuten poliisille tai palokunnalle tilanteen niin vaatiessa. Kun älykkään ovikellon, turvalaitteiden ja muiden kodin älylaitteiden yhteys internettiin on luotu, muodostavat ne yhdessä esineiden internetin. Toisin sanottuna fyysisten esineiden verkon. joka voi kerätä ja jakaa sähköistä tietoa. (Chen 2020.)

Älykotitekniikan tärkeimpiin piirteisiin kuuluu Gauravin (2018) mukaan, että se auttaa säilyttämään maapallon rajalliset resurssit. Ajan myötä ihmiset ovat yhä tietoisempia älykkään kodin tekniikoista, kun he tekevät kodistaan älykkään ja vihreän käyttämällä ohjaimia, jotka ovat integroitu osaksi kodin järjestelmiä. Älykkään kotitekniikan avulla käyttäjät voivat myös säästää energiaa säätämällä valaistusta, LVI-järjestelmiä, ikkunoiden peitteitä ja viherkasvien kastelua. Asunnon omistajat voivat käyttää järjestelmiä Internetin avulla mistä päin maailmaa tahansa.

3.1 Älykotien hyötyjä ja haittoja

Kuten monella muullakin tekniikan osa-alueella, myös älykodeista löytyy hyviä ja huonoja puolia. Hyviin puoliin kuuluu muun muassa se, että älykodit voivat tehdä elämästä helpompaa ja käytännöllisempää. Kuka ei rakastaisi tekniikka, jolla voi hallita valaistusta, viihdettä ja lämpötilaa suoraan kotisohvalta? Olitpa töissä tai lomalla älykoti voi varoittaa sinua, jos jotain tapahtuu kotonasi ja tarvittaessa hälyttää automaattisesti apua. Asukas voi herätä ilmoitukseen palohälytyksestä, kun samalla

älykoti hälyttää pelastuslaitoksen ja sytyttää valoilla polun turvaan. (Aliz 2020; Interesting Engineering 2020; Edmonds & Chandler 2021.)

Älykkäät kodit tuovat myös energiatehokkuutta. Järjestelmät kuten Z-Wave ja Zigbee asettavat joidenkin laitteiden toiminnallisuuden vähemmälle. Ne voivat mennä virransäästötilaan ja herätä kun komentoja annetaan. Sähkölaskut pienenevät, kun tyhjistä huoneista sammutetaan valot ja lämpötilaa säädetään automaattisesti sitä mukaan, kun on tarvetta. Älytalotekniikka lupaa myös valtavia etuja yksin asuville vanhuksille. Älykoti voi ilmoittaa asukkaalle, kun on aika ottaa lääkkeitä, varoittaa sairaalaa, jos asukas kaatuu pahasti ja seurata, että asukas syö tarpeeksi. Jos vanhus on hieman unohtelevainen, älykoti voi suorittaa esimerkiksi veden sulkemisen ennen kylpyammeen ylivuotoa tai sammuttaa uunin, jos kokki on vaeltanut pois. Se antaa myös muualla asuville aikuisille lapsille mahdollisuuden osallistua ikääntyvän vanhempansa hoitoon. (Aliz 2020; Interesting Engineering 2020; Edmonds & Chandler 2021.)

Se mitä huonoihin puoliin tulee, nousee ensimmäisenä esiin hinta. Asentamalla huippuluokan ominaisuudet kotiin saadaan tulokseksi korkeampi hintalappu kiinteistölle. Kaikkien niiden laitteiden hinta, mitä tarvitaan tekemään kodista älykkään, voi nousta nopeasti jopa tuhansiin euroihin, koska siihen käytetty teknologia on suhteellisen uutta. Myös niiden ylläpito voi tulla kalliiksi. Laitteiden huolto- ja korjauskustannukset nostattavat hintaa ja jossain tapauksissa uusien ominaisuuksien ja apuohjelmien lisääminen voivat myös tuoda lisää kustannuksia. (Perry, 2020; St-Pierre 2020; Lin 2021.)

Toisena huonona puolena tulee mieleen laitteiden toimintavarmuus. Tilanteessa, jossa sähköt katkeavat tai käytettävistä laitteista loppuu akku, monet kodin toiminnoista lakkaavat toimimasta. Esimerkiksi jos kodin ulko-oven älylukosta sattuu virta loppumaan, voi olla hankalaa päästä sisään kotiin tai pahemmassa tapauksessa akun loppuminen kodin turvajärjestelmästä, asettaa kodin alttiiksi murtovarkaille tai tulipalon syttyessä pelastuslaitos ei saakaan ajoissa tietoa palon alusta.

Yhtenä ongelmana on myös internet, mikä mahdollistaa sitä kautta tulevat verkkohyökkäykset. Hakkerit, jotka löytävät tavan päästä sisälle verkkoon, saattavat pystyä

sammuttamaan hälytysjärjestelmät ja valot, jolloin koti on alttiina murtautumiselle. Myös laitteiden nopea edestakainen käynnistäminen ja sammuttaminen, voi pilata osan elektroniikasta tai äärimmäisessä tapauksessa aiheuttaa jopa tulipalon. (Edmonds & Chandler 2021.)

Internettiin liittyy myös yksityisyyden huolia. Googlen päällikkö Rick Osterloh sanoi vuonna 2019, että vieraita tulisi varoittaa siitä, jos kodissa on älykäs kotilaite kuten Google Home tai Amazon Echo, koska se kuuntelee, ellei sitä ole mykistetty. Laitteiden pitäisi tallentaa vasta kuultuaan "Ok Google ..." tai "Alexa ..." mutta, joskus ne erehtyvät ja tallentavat satunnaisia keskusteluita, mitkä olisi pitänyt pysyä yksityisenä. Laitteiden tallentamat puheet voi kuunnella valmistajien omilla sovelluksilla. (Perry 2020.)

Myös Google Home -laitetta määritettäessä se on linkitettävä Google-tiliin ja käynnistettävä haku- ja puhehistoria. Tämä tarkoittaa, että kaikki Google-haut puhelimestasi ja tietokoneeltasi olettaen, että ne tehdään kirjautuneena, tallennetaan. Toisaalta, jos hakuhistorian ottaa pois käytöstä myöhemmin, se tekee kotilaitteestasi periaatteessa käyttökelvottoman. Myös älykkäisiin kameroihin ja ovikelloihin voidaan murtautua, ja sitä kautta pääsee tarkastelemaan näitä yksityisiä videosyötteitä kaikkialla maailmassa. Suurimmasta hyödystä eli kyvystä valvoa kotiasi etäältä, tulee sen suurin heikkous. (Perry 2020.)

3.2 Lyhyt katsaus älykodin historiaan

Älykoti ei ole uusi luomus. Se on ollut yleistä konseptin muodossa kuluttajien ja alan asiantuntijoiden keskuudessa. Älykoti -konsepti alkoi kauko-ohjainten keksinnöllä, jonka Nikola Tesla (1856–1943) paljasti vuonna 1898. 1900-luvun alussa todistettiin teollista vallankumousta, joka avasi tietä ensimmäisten kodinkoneiden käyttöönotolle. Vuonna 1901 esiteltiin ensimmäinen pölynimuri, jota seurasivat kuivausrummut, pesukoneet, jääkaapit ja sähköiset astianpesukoneet. Nämä eivät olleet ”älykkäitä” laitteita, mutta mullistivat ihmisten elämän 1900-luvulla. (Gaurav 2018.)

1930-luvulla keksijät kiinnittivät huomionsa kotiautomaatiotekniikoihin, mutta idea toteutui vasta vuonna 1966, jolloin kehitettiin ensimmäinen älykäs automaatiojärjestelmä Echo IV, jonka kehitti Westinghouse-insinööri James Sutherland. Tämän laitteen avulla kuluttajat pystyivät luomaan laskennallisia ostoslistoja, hallita kodin lämpötilaa ja kytkeä laitteita päälle ja pois päältä. Samalla vuosikymmenellä vuonna 1969 aloitti todellinen yhdistettyjen laitteiden maailmankaikkeus ARPAnet, joka on nykypäivän internetin edeltäjä. (Gaurav 2018; Zeus Integrated 2019.)

Älykotitekniikan nykyaikainen alku voidaan jäljittää vuoteen 1975, jolloin julkaistiin X10, kotiautomaatioalusta, joka lähettää digitaalista tietoa radiotaajuisten purskeiden kautta kodin olemassa oleviin sähköjohdotuksiin. Tämän tekniikan avulla pystyttiin hallitsemaan kodin valaisimia ja pieniä laitteita. Kun vuosikymmen vaihtui 1980-luvun puolelle se toi tullessaan suuria muutoksia kuluttajalle. Liiketunnistavat valot, automaattiset autotallin oven avaajat, ohjelmoitavat termostaatit ja turvajärjestelmät olivat nyt yleisiä ja edullisia. Vuonna 1984 Amerikan kodinrakentajien liitto otti käyttöön termin "älykäs talo". (Zeus Integrated 2019; Stanley 2021.)

Vuonna 1990 Interop Internet -verkkoshow'n johtaja Dan Lynchin esittämä haaste johti siihen, että John Romkey ja Simon Hackett loivat leivänpaahtimen, joka oli yhteydessä Internetiin ja sitä pystyttiin ohjaamaan sen kautta. Esineiden internet (IoT) oli syntynyt. 2000-alkupuolella vuonna 2005 otettiin käyttöön Z-Wave-alusta, joka käyttää radiotaajuutta älykotitekniikkaan. Se toimii alle 1 GHz: n taajuudella, johon ei vaikuta Wi-Fin ja muiden langattomien tekniikoiden, kuten Bluetoothin, aiheuttamat häiriöt. Tuotteet, joissa on sisäänrakennettu Z-Wave, muodostavat mesh-verkon ja voivat etä-kommunikoida laitteesta toiseen. Asunnon omistajat voivat myös lisätä muita kuin Z-Wave-tuotteita verkkoonsa kytkemällä ne Z-Wave-lisävarustemoduuleihin. (Zeus Integrated 2019; Stanley 2021.)

Älylaitteet ja -järjestelmät ovat kehittyneet nopeasti 2000-luvulla. Arvioiden mukaan vuoteen 2012 mennessä käytössä oli jo 1,5 miljoonaa automaattista kotijärjestelmää. Vuonna 2014 Amazon esitteli Prime-jäsenilleen Amazon Echon, ja vaikka sitä alun perin markkinoitiin ääniohjatulla musiikkiratkaisuna, Alexan sisällyttäminen osoitti nopeasti laitteen käytön älykkään kodin keskuksena. Tänä päivänä IoT-laitteita on paljon enemmän kuin koskaan, ja älykkäiden kotijärjestelmien kustannukset laskevat

jatkuvasti, mikä tekee niistä houkuttelevan vaihtoehdon asunnon omistajille. Kotiautomaatioteollisuus on kuitenkin kärsinyt kasvukivuista omien ohjelmistojen ja järjestelmien takia. Usein kuluttajilla on vaikeuksia valita haluamiensa laitteiden ja saumattoman asennuksen väliltä. (Zeus Integrated 2019.)

Ihmisluontoon kuuluu löytää tapoja, jotka tekevät arjesta helpompaa ja miellyttävämpää. Kotiautomaatio, mikä on käytännössä älykkään kodin edeltäjä, herätettiin elämään tekniikan kehityksen kautta, erityisesti Internetin ja tietokoneen avulla. 1950-luvun tieteiskirjallisuus kuvasi ensimmäisiä näkemyksiä kodeista, joita koneet valvovat ja ohjaavat täysin automaattisesti. Vuonna 1999 Disney-elokuvassa ”Smart House” kerrottiin kotitietokoneista ja sen seurauksista, kun älykoneet alkoivat elää omaa elämäänsä. Disney osoittautui tahattomasti visionääriseksi elokuvan osassa, jossa talon älykäs ohjausyksikkö kehittää mustasukkaisuuden tunteen. Todellisuudessa tulee todennäköisesti kestämään muutama vuosi ennen kuin koneet voivat "tuottaa" tunteita. (Infineon 2017.)

Tutkijat ovat työskennelleet jo yli 30 vuoden ajan kodinkoneiden yhdistämisen ja niiden käytön automatisoinnin parissa. Silti vain viimeiset 15 vuotta älykäs koti on herättänyt laajaa yleistä kiinnostusta. Tärkeimpinä syinä ovat nykyiset haasteet, kuten yhteiskunnan ikääntyminen, lisääntynyt ympäristötietoisuus ja siihen liittyvä halu saada aikaan kestävä energiansaanti. Digitaalisen toiminnan lisääminen ja uudet keinot parantaa mukavuutta keskuudessamme olivat myös tekijöitä, jotka asettivat älykkään kodin yleisen edun keskiöön vuosituhannen vaihteessa. (Infineon 2017.)

4 YHTEYSTYYPIT

Yhteystyypit ovat tärkeä osa IoT:n maailmaa. Ne mahdollistavat laitteiden yhdistymisen internettiin ja sitä kautta maailmalle. Yhteystyyppejä on montaa erilaista, mutta tähän kappaleseen olen kerännyt omasta mielestäni oleellisemmat yhteystyypit. Oikean yhteystyypin valinta riippuu siitä, mihin ja missä IoT laitteita tullaan käyttämään. Eri tyypeillä on erilaisia ominaisuuksia ja kaikista löytyy hyvät ja huonot puolensa.

Yhteystyypeissä *langaton tekniikka* on käytännössä pakollinen. Jos laitteet kytkettäisiin johdoilla, olisi niitä tuhansia, ellei miljoonina kilometrejä lisää jo olemassa olevien johtojen rinnalle. Langaton tekniikka mahdollistaa myös esineiden liikkumisen. Se mahdollistaa robotti-imurin siirtymisen huoneesta toiseen ja sen ohjaamisen puhelimella, vaikka toiselta puolelta kaupunkia.

Mobiiliverkkojen kehittyminen nykytasolle on suurimpia syitä IoT:n laajalle leviämiselle. Jokaisen uuden sukupolven myötä tiedonsiirtonopeudet kasvavat ja viive pienenee, mikä mahdollistaa yhä suurempia tietopakettien siirtämisen lähettimestä vastaanottimeen. Samalla se mahdollistaa tiedon siirtämisen myös liikkeellä. Ei tarvitse olla kahvilan Wi-Fin kuuluvuusalueella, että saisi saunan lämpimäksi ennen kotiin tuloa.

Bluetoothin ja *NFC:n* tuleminen mahdollisti laitteiden nopeamman ja helpomman yhdistämisen ja nopean tiedonsiirron pienelle määrälle dataa. NFC:tä käyttämällä pystyy esimerkiksi maksamaan ostoksensa kännykällä tai lähettämään kuvan kaverille pelkästään laittamalla puhelimet tai laitteet lähekkäin. Bluetooth puolestaan on tehnyt helpoksi yhdistää kaiuttimia tai langattomia kuulokkeita. Ei tarvitse muuta kuin laittaa Bluetooth päälle, etsiä laite ja yhdistää. Yhteys jää muistiin, mikä tarkoittaa sitä, että yhdistetyt laitteet tulevat saman kuuluvuusalueen sisällä, muodostamaan yhteyden automaattisesti.

4.1 Mobiiliverkot

Pääsy 3G-yhteyksiin oli mahdollista ensimmäisen kerran vuonna 2001, jolloin voimme käyttää puhelintamme muuhunkin kuin vain puheluita ja viestejä varten. Tämä avasi mahdollisuuden netin selaamiseen, sähköpostiviestien lähettämiseen ja median jakamiseen tien päällä. 3G-verkon nopeuden on oltava vähintään 200 kbps jotta se voidaan luokitella sellaiseksi. (TravelWifi 2019)

Vuonna 2009 saapui seuraavan sukupolven älypuhelinteknologiaa, 4G-yhteensopivat laitteet ja 4G-verkko. Verkko ei ollut kuitenkaan kovin yleinen tässä vaiheessa, joten yhdistyminen tapahtui vielä 3G-verkossa. Kuten voit arvata, 4G oli pohjimmiltaan 3G:n nopeampi versio. 4G-yhteys vaihtelee 100 mbps ja 1gbps välillä. Kilobitin ja gigabitin ero on valtava, joten tämä vastasi uskomattomia nopeuksia, vaikka useimmat verkot eivät saavuttaneet tätä ylärajaa. Toisen eron 3G:n ja 4G:n välillä oletetaan olevan yhteyden turvallisuuden ja luotettavuuden parantaminen. (TravelWifi 2019)

Seuraavan sukupolven tietoliikenneverkot, jota kutsutaan viidenneksi sukupolveksi tai 5G:si on alkanut saapua markkinoille vuoden 2018 lopussa ja jatkavat laajentumistaan maailmanlaajuisesti. Nopeuden parantamisen lisäksi tekniikan odotetaan vapauttavan massiivisen 5G IoT ekosysteemin, jossa verkot voivat palvella miljardien yhdistettyjen laitteiden viestintätarpeita nopeuden, viiveen ja kustannusten välillä sopivin kompromissein. (Thales 2021.)

Yksi suurimmista eroista 4G:n ja 5G:n välillä on huippukapasiteetti ja viive. Esimerkiksi 5G UWB-sektorin huippukapasiteetti on gigabittiä sekunnissa verrattuna 4G:n megabittiä sekunnissa. Myös viive tai aika, joka kuluu siitä hetkestä, kun tiedot lähetetään laitteelta, kunnes vastaanotin käyttää sitä, vähenee huomattavasti 5G-verkoissa, mikä mahdollistaa nopeamman lähetys- ja latausnopeuden. Toinen suuri ero 4G:n ja 5G:n välillä on kaistanleveyden koko. 5G:n pitäisi pystyä tukemaan monia muita tulevaisuuden laitteita liitettyjen ajoneuvojen ja muiden esineiden internetissä olevien laitteiden verkkovaatimusten lisäksi. (Gwaltney 2018; Verizon 2019.)

		3G	4G	5G
	Deployment	2004-05	2006-10	2020
	Bandwidth	2mbps	200mbps	>1gbps
	Latency	100-500 milliseconds	20-30 milliseconds	<10 milliseconds
	Average Speed	144 kbps	25 mbps	200-400 mbps

Kuva 3. 3G:n, 4G:n ja 5G:n nopeuseroja. (Vella 2019.)

4.2 Bluetooth

Bluetooth lähettää ja vastaanottaa radioaaltoja 79 eri taajuudella eli kanavalla, joiden keskipiste on 2,45 GHz, mikä erottaa sen radiosta, televisiosta ja matkapuhelimista. Bluetoothissa on lyhyen kantaman lähettimet, minkä ansiosta ne eivät kuluta käytännössä ollenkaan virtaa ja koska kantama on lyhyt, ne ovat teoriassa turvallisempia kuin pidemmillä matkoilla toimivat langattomat verkot, kuten Wi-Fi. (Woodford 2020.)

Bluetooth-laitteet tunnistavat toisensa ja luovat yhteyden automaattisesti ja jopa kahdeksan niistä voi kommunikoida kerralla. Ne eivät häiritse toisiaan, koska jokainen laitepari käyttää omaa kanavaa kaikista 79 käytettävissä olevasta kanavasta. Jos kaksi laitetta haluaa puhua keskenään, ne valitsevat kanavan satunnaisesti ja, jos kanava on jo otettu, ne siirtyvät satunnaisesti toiseen kanavaan. Tämä tekniikka tunnetaan nimellä hajaspektritaajuushyppely. Minimoidakseen muiden sähkölaitteiden aiheuttamat häiriöriskit, laiteparit vaihtavat jatkuvasti käyttämäänsä taajuutta jopa tuhansia kertoja sekunnissa. (Nield 2016; Woodford 2020.)

Bluetoothia on kahta erilaista, Bluetooth Basic Rate / Enhanced Data Rate (BR / EDR) ja Bluetooth Low Energy (LE). Bluetooth BR / EDR on rajoitetumpi kantaman suhteen, mutta se soveltuu paremmin jatkuvan yhteyden ylläpitoon, esimerkiksi äänen suoratoistoon. Bluetooth LE:llä on enemmän mahdollisuuksia esineiden internetiin,

missä tarvitaan lyhyempiä tietopurskeita ja joissa virran säästö on tärkeämpää. Se on myös halpa toteuttaa, minkä vuoksi se onnistui löytämään tiensä niin moniin kuluttajalaitteisiin. (Nield 2016.)

4.3 Zigbee

Zigbee on langaton tekniikka, joka on kehitetty avoimeksi globaaliksi standardiksi vastaamaan edullisten, pienitehoisten langattomien IoT-verkkojen ainutlaatuisiin tarpeisiin. Zigbee-standardi toimii IEEE 802.15.4 fyysisen radiospesifikaation mukaisesti ja toimii lisensoimattomilla taajuuksilla, mukaan lukien 2,4 GHz, 900 MHz ja 868 MHz. (Digi 2021.)

Zigbee on lyhyen kantaman tiedonsiirtostandardi, kuten Bluetooth ja Wi-Fi, joka kattaa 10–100 metrin kantaman. Erona on, että Bluetooth ja Wi-Fi tukevat monimutkaisten rakenteiden, kuten median, ohjelmistojen jne. siirtämistä, kun taas Zigbee tukee yksinkertaisten tietojen siirtämistä antureista. Se tukee matalaa, noin 250 kbps:n datansiirtonopeutta. Zigbee tekniikkaa käytetään pääasiassa sovelluksiin, jotka vaativat vain vähän virtaa, alhaisia kustannuksia ja tiedonsiirtonopeuksia, sekä pitkän akun käyttöiän. (Electrical Technology 2021.)

Laitteiden tai niin kutsuttujen solmujen enimmäismäärä samassa Zigbee-verkossa on 65000, joten mikään tavallinen koti ei saavuta Zigbee-verkon rajoituksia. Zigbee-laitteet muodostavat yhteyden joko omaan keskittimeen, kuten Hue Bridgeen, tai kolmannen osapuolen älykkään kodin keskittimeen, kuten Samsung SmartThings Hubiin. Alkuperäinen ja toisen sukupolven Amazon Echo Plus sisältää myös Zigbee-sirun, joten sillä voi muodostaa yhteyden suoraan joihinkin älykkäisiin kodin laitteisiin tarvitsematta keskittimiä tai Wi-Fi-siltoja. (Charlton 2020.)

4.4 Z-Wave

Z-Wave toimii taajuusalueella 800–900 MHz. Tämä tarkoittaa, että toisin kuin Zigbee, Z-Wave ei toimi 2,4 GHz:n taajuudella, jota Wi-Fi käyttää. Koska tämä taajuus on poissa käytöstä, Z-Wave välttää mahdolliset häiriöt lähellä olevista Wi-Fi-laitteista. (Charlton 2020.)

Todellinen taajuus, jolla Z-Wave-laitteet toimivat, riippuu maasta, jossa sitä käytetään. Esimerkiksi Yhdysvallat käyttää 908,40 MHz:n, 908,42 MHz:n ja 916 MHz:n taajuuksia, kun taas Yhdistynyt Kuningaskunta ja Eurooppa käyttävät 868,40 MHz:n, 868,42 MHz:n ja 869,85 MHz:n taajuuksia. On tärkeää varmistaa, että ostamasi Z-Wave-laite on suunniteltu alueellesi. (Lamkin 2021.)

Jokaisella Z-Wave-verkolla on yksilöllinen 32 bittinen tunnus, joka varmistaa, että eri verkkojen laitteet eivät voi puhua keskenään. Yksittäisen verkon jokaiselle laitteelle annetaan myös yksilöllinen 8 bittinen solmutunnus ja yksittäinen verkko sallii jopa 232 erillistä laitetta. Laitteet lisätään Z-Wave-verkkoon prosessissa, jota kutsutaan "sisällyttämiseksi", joka jakaa niille verkkotunnuksen, lisää salausavaimet ja kartoittaa signaalin voimakkuuden läheisiin laitteisiin viestien reititystä varten. (Mead 2020.)

Kuten Zigbee, Z-Wave käyttää paljon vähemmän virtaa kuin muut langattomat tekniikat, kuten Wi-Fi ja Bluetooth, mikä tarkoittaa, että laitteiden akut vaihtuvat harvoin, joissakin tapauksissa vain kerran 10 vuodessa. Toisin kuin Wi-Fi ja Bluetooth, Z-Wave on suunniteltu kuljettamaan vain pieniä määriä dataa, kuten ohjeita ja tietoja laitteista, kuten liiketunnistimista. Sillä ei ole valtavaa Wi-Fi-kaistanleveyttä, mutta se ei ole välttämätöntä, kun Z-Wave-kytkin pyytää älykästä hehkulamppua käynnistymään. (Charlton 2020.)

4.5 NFC

Near Field Communication (NFC) on kosketuksettomaan viestintätekniikkaan perustuva radiotaajuuskenttä (RF), joka käyttää 13,56 MHz:n perustaajuutta. NFC-tekniikka on suunniteltu täydellisesti tietojen vaihtamiseen kahden laitteen välillä yksinkertaisella kosketuseleellä. (NFC Forum 2021.)

NFC perustuu RFID-tekniikkaan eli radiotaajuiseen etätunnistukseen. RFID-järjestelmät käsittävät ainakin yhden initiaattorin, eli tyypillisesti RFID-luku- / kirjoituslaitteen ja minkä tahansa määrän kohdelaitteita, jotka tunnetaan transpondereina Ne vastaanottavat, käsittelevät ja vastaavat initiaattorilta vastaanotettuihin viesteihin. Tiedonsiirto tapahtuu sähkömagneettisen induktion avulla kahden silmukka-antennin välillä. RFID-lukulaitteen ja transponderin välistä rakoa kutsutaan ilmarajapinnaksi. RFID-tekniikan tarkoituksena on tunnistaa, todentaa ja jäljittää esineitä tai ihmisiä. Esimerkiksi logistiikassa RFID-lähetinlaitteet on kiinnitetty tuotteisiin tai kuljetuslavoihin tavaravirran seuraamiseksi. (Ionos 2020)

NFC tarjoaa kontaktitonta yhteyttä noin 4 tai 5 senttimetrin etäisyydelle. Tällä tavoin tietoliikenne on luonnostaan turvallisempaa, koska laitteet ovat tavallisesti kosketuksissa vain siten, kun käyttäjä näin päättää. NFC on RFID-muoto, mutta sillä on erityiset standardit, jotka säätelevät sen toimintaa ja käyttöliittymää. Tämä tarkoittaa, että NFC-laitteita ja useiden valmistajien elementtejä voidaan käyttää yhdessä. NFC-standardit määräävät kontaktittoman toimintaympäristön lisäksi myös datamuodot ja tiedonsiirtonopeudet. (Electronics notes 2021)

5 TIETOTURVA JA YKSITYISYYS

IoT yhdistää yhä enemmän laitteita ja olemme menossa kohti maailmaa, jossa on 64 miljardia laitetta yhdistettynä internetiin vuoteen 2025 mennessä (Business Insider 2020). Nopealla kasvulla on useita etuja, koska se muuttaa tapaa, jolla ihmiset suorittavat päivittäisiä tehtäviä. Älykodin hankkiminen on epäilemättä hienoa, ja se voi samalla vähentää energian kokonaiskulutusta ja pienentää sähkölaskua.

Uusi kehitys mahdollistaisi kytkettyjen autojen yhdistämisen älykaupungin infrastruktuuriin luodakseen kuljettajalle täysin erilaisen ekosysteemin, joka on tottunut perinteiseen tapaan kulkemaan a:sta b:hen. Kytketyt terveydenhuollon laitteet antavat

ihmisille syvemmän ja kattavamman kuvan omasta terveydestään tai sen puutteesta kuin koskaan ennen. Mutta näillä kaikilla eduilla on riskinsä, koska kytkettyjen laitteiden lisääntyminen antaa hakkereille ja kyberrikollisille enemmän kohteita. (Business Insider 2020; Peterson 2021.)

Vuonna 2015 ryhmä hakkereita otti sähköverkon pois päältä Länsi-Ukrainassa aiheuttaakseen ensimmäisen sähkökatkoksen, joka on tehty kyberrikollisten toimesta. Ja tämä on todennäköisesti vasta alkua, koska nämä hakkerit etsivät lisää tapoja hyökätäkseen kriittisiin infrastruktuureihin kuten sähkö- ja vesivoimalaitoksiin. (Business Insider 2020.)

5.1 Tietoturvan ongelmia

Tietoturvan ongelmana on yleinen käsitys IoT:sta. Jos IoT lähtee koskaan leviämään laajalle, yleisen käsityksen on oltava ensimmäinen ongelma, johon valmistajien on puututtava. IControllin tekemän 2015 *state of the smart home* -raportin mukaan 44 % kaikista amerikkalaisista oli ”erittäin huolissaan” mahdollisuudesta, että heidän tietonsa varastetaan heidän älykodistaan ja 27 % oli ”jonkin verran huolissaan”. Tämän huolenaiheen vuoksi kuluttajat epäröivät ostaa IoT-laitteita. (Business Insider 2020.)

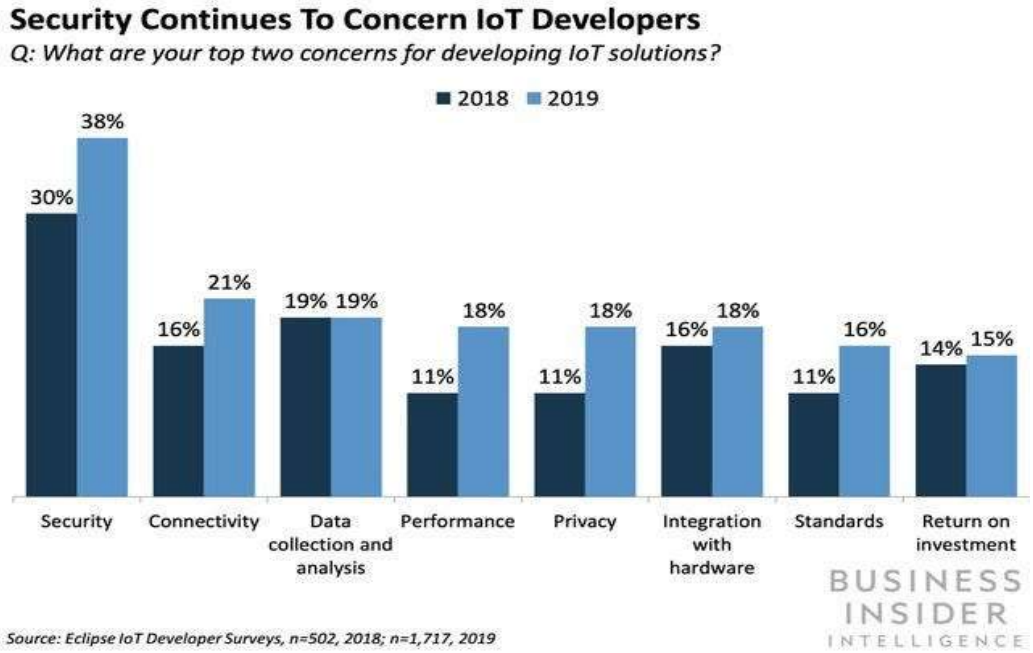
Toisena ongelmana tulee haavoittuvuudet. Ne ovat suurin ongelma, joka vaivaa jatkuvasti käyttäjiä ja organisaatioita. Yksi tärkeimmistä syistä, miksi IoT-laitteet ovat haavoittuvia on se, että niillä ei ole sisäänrakennettua laskentatehoa suojaukseen. Toinen syy siihen, miksi haavoittuvuudet voivat olla niin yleisiä, on rajallinen budjetti suojatun laiteohjelmiston kehittämiseen ja testaamiseen, mihin vaikuttavat laitteiden hintataso ja niiden erittäin lyhyt kehitysjakso. Protokollat, kuten HTTP (Hypertext Transfer Protocol) ja API (Application Programming Interface), ovat vain muutamia kanavista, joihin IoT -laitteet luottavat ja joita hakkerit voivat käyttää. (Sembera & Urbanec 2021; Shea 2021.)

Kolmantena ongelmana ovat haittaohjelmat. Huolimatta useimpien IoT -laitteiden rajallisesta laskentakapasiteetista, niihin voi silti tartuttaa haittaohjelmia. Tämä on asia, jota verkkorikolliset ovat käyttäneet tehokkaasti viime vuosina. *IoT botnet* -

haittaohjelmat ovat yleisimmin nähtyjä variantteja, koska ne ovat sekä monipuolisia että kannattavia tietoverkkorikollisille. Merkittävin hyökkäys oli vuonna 2016, jolloin Mirai-botnet poisti käytöstä suuret verkkosivustot ja palvelut käyttäen tavallisia IoT-laitteita. Muita haittaohjelmaperheitä ovat kryptovaluuttalouhintaan tarkoitetut haittaohjelmat ja lunnasohjelmat. (Sembera & Urbanec 2021.)

Neljäntenä on lisääntyneet kyberhyökkäykset. Tartunnan saaneita laitteita käytetään usein hajautettujen palvelunestohyökkäysten (DDoS) hyökkäyksiin. Kaapattuja laitteita voidaan käyttää myös hyökkäyspohjana useiden koneiden saastuttamiseen ja haitallisen toiminnan peittämiseen. Vaikka organisaatiot voivat vaikuttaa kannattavammilta kohteilta, älykkäät kodit näkevät myös yllättävän paljon odottamattomia kyberhyökkäyksiä. (Sembera & Urbanec 2021.)

Viimeisenä on laitteen virheellinen hallinta ja virheellinen kokoonpano. Turvallisuuden valvonta, huono salasanan hygienia ja yleinen laitteen huono hallinta voivat auttaa näiden uhkien onnistumisessa. Käyttäjiltä voi myös yksinkertaisesti puuttua tietämystä ja kykyä toteuttaa asianmukaisia turvatoimenpiteitä, jolloin palveluntarjoajien ja valmistajien on ehkä autettava asiakkaitaan saamaan parempi suoja. (Sembera & Urbanec 2021.)



Kuva 8. Kuvassa on Business Insiderin kyselyn tulokset (Business insider 2020.)

5.2 Yksityisyyden ongelmia

IoT:n vaarallisin osa on se, että kuluttajat luopuvat yksityisyydestään vähitellen edes huomaamatta sitä, koska he eivät ole tietoisia siitä, mitä tietoja kerätään ja miten niitä käytetään. Koska mobiilisovellukset, puettavat laitteet ja muut Wi-Fi-yhteydellä varustetut kuluttajatuotteet korvaavat markkinoilla olevat "tyhmät" laitteet, ei kuluttajalla ole mahdollisuutta ostaa tuotetta ilman seurantaa. On normaalia, että kuluttajat päivittävät laitteitaan, eikä heille todennäköisesti tule mieleen, että nämä uudet laitteet myös valvovat heitä.

Vuosien mittaan Internetin käyttäjät ovat oppineet välttämään roskapostia tai tietojenkalasteluviestejä, suorittamaan virustarkistuksia tietokoneilleen ja suojaamaan Wi-Fi-verkkonsa vahvoilla salasanoilla. Mutta IoT on uusi tekniikka, ja ihmiset eivät vieläkään tiedä paljoa siitä. Vaikka suurin osa IoT:n turvallisuusongelmien riskeistä on edelleen valmistuksen puolella, käyttäjät ja liiketoimintaprosessit voivat luoda suurempia uhkia. Yksi suurimmista IoT:n tietoturvariskeistä ja -haasteista on käyttäjän tietämättömyys ja tietoisuuden puute IoT -toiminnoista. Tämän seurauksena kaikki ovat vaarassa. (Intellectsoft 2020.)

Yhteiskuntatekniikkaa käytettiin vuoden 2010 Stuxnet -hyökkäyksessä Iranin ydinlaitosta vastaan. Hyökkäys kohdistettiin teollisiin ohjelmoitaviin logiikkaohjaimiin (PLC), jotka kuuluvat myös IoT -laiteluokkaan. Hyökkäys korruptoi 1000 sentrifugia ja sai laitoksen räjähtämään. Uskotaan, että sisäinen verkko eristettiin julkisesta verkosta hyökkäysten välttämiseksi, mutta tarvittiin vain yksi työntekijä kytkemään USB-muistitikku yhteen sisäisistä tietokoneista. (Intellectsoft 2020.)

Yhtenä isona ongelmana on myös datan määrä. Suuret tietomäärät, joita IoT -laiteet voivat tuottaa, ovat huikeita. Liittovaltion kauppakomission raportissa "Internet of Things: Privacy & Security in a Connected World" todettiin, että vähemmän kuin 10 000 kotitaloutta voi tuottaa 150 miljoonaa erillistä datapakettia päivittäin. Tämä luo hakkereille enemmän mahdollisuuksia ja jättää arkaluontoiset tiedot haavoittuviksi. (Business Insider 2020.)

Toisena ongelmana on ei toivottu julkinen profiili. Olet epäilemättä hyväksynyt palvelusehdot jossain vaiheessa, mutta oletko koskaan lukenut koko asiakirjaa? Edellä mainitussa liittovaltion kauppakomission raportissa todettiin, että yritykset voisivat käyttää kerättyä tietoa, jota kuluttajat tarjoavat vapaaehtoisesti työllistämispäätösten tekemiseen. Esimerkiksi vakuutusyhtiö voi kerätä tietoja internettiin kytketystä autosta kuljettajan ajotavoista laskiessaan vakuutusturvaa. Sama voi tapahtua terveys- ja henkivakuutuksissa seuraamalla asiakkaan terveyttä urheilukellojen avulla. (Business Insider 2020.)

6 POHDINTA

Tämän opinnäytetyön tarkoituksena oli tutustua esineiden internetin maailmaan. Tutkiessani asiaa huomasin, kuinka laaja ja monipuolinen kyseinen tekniikan osa-alue on, joten päätin supistaa aluetta ja keskittyä pelkästään älykkäisiin koteihin. Minua on aina kiinnostanut älykkään kodin ratkaisut. Esimerkiksi nykyaikainen valaistus, jota pystytään ohjaamaan etäältä, tai että sen saa automatisoitua seuraamaan käyttäjänsä liikkeitä, tai kun käyttäjä saapuu kotiin, niin sen seurauksena valot syttyvät. Toisena esimerkkinä on turvallisuus, jolloin saat ilmoituksia kännykkääsi, jos joku murtautuu kotiisi tai siellä syttyy tulipalo. Ilmoitukset näistä asioista lähtevät automaattisesti niitä valvoville asianomaisille.

Nykypäivänä esineiden internet on kovassa kasvussa ja leviää ympäri maailmaa. Kun kehitykseen osallistuvat suuret nimet kuten Google, Apple, Amazon ja Microsoft, uskon että IoT:n kehitys monin kertaistuu lähitulevaisuudessa. Kehityksen myötä tulee myös ongelmia, jotka kaipaavat ratkaisuja, kuten esimerkiksi yksityisyyden suoja ja tietoturva. Edellä mainitut suuret yritykset ovat tunnettuja siitä, että heidän yksityisyyden suojansa on kyseenalainen, vaikka heidän tietoturvansa on maailman kärkeä. Myös monella kodinkonevalmistajalla tuntuu olevan ongelmia tietoturvan kanssa. Esimerkkinä voidaan käyttää robotti-imuria, minkä pystyy hakkeroiman ja imurin kameraa voidaan käyttää ihmisten vakoilemiseen.

Uskon, että tulevaisuudessa näitä suurempia ongelmia saadaan ratkaistua ja esineiden internet tulee mullistamaan maailman, varsinkin nyt, kun 5G-teknologia alkaa yleistymään ja uudempia teknologeja kehitetään koko ajan. Valmistajien tarvitsisi tehdä enemmän yhteistyötä keskenään ja rakentaa yhteisiä standardeja asian edistämiseen. Uskon, että tulevaisuuden kodeissa tulee olemaan vakiokalustona jonkinnäköinen keskitetty älykotiratkaisu, jota pystyy ohjaamaan etäältä ja joka pystyy seuraamaan käyttäjänsä rutiineja ja tekemään ratkaisuja sen mukaan. Yhtä kaikki, tulevaisuus esineiden internetille näyttää valoisalta.

LÄHTEET

Aliz, D. Advantages and Disadvantages of Smart Home Technology. Viitattu 19.04.2021. https://www.upscalelivingmag.com/advantages-and-disadvantages-of-smart-home-technology/

Burgess, M. 2018. What is the Internet of Things? WIRED explains. Viitattu 20.03.2021. https://www.wired.co.uk/article/internet-of-things-what-is-explained-iot

Business Insider. 2020. The security and privacy issues that come with the internet of things 06.01.2020. https://www.businessinsider.com/iot-security-privacy?r=US&IR=T

Charlton, A. 2020. What is Z-Wave and how does it work to automate my smart home? Viitattu 02.03.2021. https://www.gearbrain.com/what-is-z-wave-technology-2597781116.html

Chen, J. 2020. Smart Home. Viitattu 27.03.2021. https://www.investopedia.com/terms/s/smart-home.asp

Digi. 2021. Zigbee Wireless Mesh Networking. Viitattu 02.03.2021. https://www.digi.com/solutions/by-technology/zigbee-wireless-standard

Edmonds, M & Chandler, N. 2021. How Smart Homes Work. Viitattu 19.04.2021. https://home.howstuffworks.com/smart-home.htm

Electrical Technology. 2021. What is Zigbee Technology and How it works. Viitattu 02.03.2021. https://www.electricaltechnology.org/2017/09/zigbee-technology-wireless-networking-system.html

Electronics notes. 2021. What is NFC: near field communication. Viitattu 02.03.2021. https://www.electronics-notes.com/articles/connectivity/nfc-near-field-communication/what-is-nfc-tutorial.php

Gaurav, S. 2018. The Evolution of Smart Home Technology. Viitattu 27.03.2021. https://blog.bccresearch.com/the-evolution-of-smart-home-technology

Gillis, A. 2020. Internet of Things (IoT). Viitattu 20.03.2021. https://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT

Gwaltney, H. 2018. Difference between 3G, 4G LTE and 5G VoLTE: What it all means. Viitattu 04.03.2021. https://gtb.net/why-gtb/blog/difference-between-3g-4g-lte-and-5g-volte-what-it-all-means

Infineon. 2017. Smart Home: Everything you need to know. Viitattu 27.03.2021. https://www.infineon.com/cms/en/discoveries/smart-home-basics/

Intellectsoft. 2020. Top 10 Biggest IoT Security Issues. Viitattu 02.09.2021. https://www.intellectsoft.net/blog/biggest-iot-security-issues/

Interesting Engineering. 2020. 7 Advantages of Using Smart Home. Viitattu 19.04.2021. https://interestingengineering.com/7-advantages-of-using-smart-home-technologies

Ionos. 2020. What is NFC? Functions Provided by Near-Field Communication. Viitattu 02.03.2021. https://www.ionos.com/digitalguide/server/know-how/nfc-near-field-communication/

Khvoynitskaya, S. 2019. How can your company benefit from IoT data analytics? Viitattu 20.03.2021. https://www.itransition.com/blog/iot-data-analytics

Lamkin, P. 2021. Z-Wave explained: What is Z-Wave and why is it important for your smart home? Viitattu 02.03.2021. https://www.the-ambient.com/guides/zwave-z-wave-smart-home-guide-281

Lin, P. 2021. Disadvantages of a Smart Home. Viitattu 25.04.2021. https://www.hunker.com/12435186/disadvantages-of-a-smart-home

McClelland, C. 2020. What is IoT? A simple explanation of the internet of things. Viitattu 20.03.2021. https://www.iotforall.com/what-is-iot-simple-explanation/

Mead, D. 2020. A Comprehensive Guide to Z-Wave. Viitattu 02.03.2021. https://linkdhome.com/articles/What-is-z-wave

Meola, A. 2021. A look at examples of IoT devices and their business applications in 2021. Viitattu 20.03.2021. https://www.businessinsider.com/internet-of-things-devices-examples?r=US&IR=T

NFC-Forum. 2021. What is NFC: About the Technology. Viitattu 02.03.2021. https://nfc-forum.org/what-is-nfc/about-the-technology/

Nield, D. 2016. What is Bluetooth? Viitattu 03.03.2021. https://www.techradar.com/how-to/computing/what-is-bluetooth-1323284

Perry, T. 2020. Why Are Smart Homes “Bad”? 19 Disadvantages to Consider. Viitattu 25.04.2021. https://www.smarthomepoint.com/disadvantages/

Peterson, J. 2021. The Internet of Things Is Everywhere. Are You Secure? Viitattu 01.09.2021. https://www.whitesourcesoftware.com/resources/blog/iot-security/

Ranger, S. 2020. What is the IoT? Everything you need to know about the Internet of Things right now. Viitattu 20.03.2021. https://www.zdnet.com/article/what-is-the-internet-of-things-everything-you-need-to-know-about-the-iot-right-now/

Ryynänen, T. 2016. Tekniikkaa ja taloutta. Viitattu 26.01.2020. https://blogit.haaga-helia.fi/ryynanen/2016/02/29/mita-internet-of-things-voi-tarkoittaa-selkokielella/

Sembera, V. & Urbanec, J. 2021. IoT Security Issues, Threats and Defenses. Viitattu 01.09.2021. https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/iot-security-101-threats-issues-and-defenses

Shea, S. 2020. Smart home or building (home automation or domotics). Viitattu 27.03.2021. https://internetofthingsagenda.techtarget.com/definition/smart-home-or-building

Shea, S. 2021. IoT security (internet of thigs security). Viitattu 01.09.2021. https://internetofthingsagenda.techtarget.com/definition/IoT-security-Internet-of-Things-security

Shoemaker, C. 2019. IoT Data: How to Collect, Process, and Analyze Them.Viitattu 20.03.2021. https://www.toolbox.com/tech/iot/blogs/iot-data-how-to-collect-process-and-analyze-them-032619/

Stanley, J. 2021. The History of Smart home Technology. Viitattu 27.03.2021. https://www.familyhandyman.com/article/the-history-of-smart-home-technology/

St-Pierre, D. 2020. The Benefits and Disadvantages of Home Automation. Viitattu 25.05.2021. https://iamdanielstp.com/the-benefits-and-disadvantages-of-home-automation/

Thales. 2021. Introducing 5G technology and networks (speed, use cases and rollout). Viitattu 04.03.2021. https://www.thalesgroup.com/en/markets/digital-identity-and-security/mobile/inspired/5G

TravelWifi. 2019. What Is the Difference Between 3G, 4G & 5G Networks. Viitattu 04.03.2021. https://travelwifi.com/blog/en/difference-3g-4g-5g-networks/

Vella, H. 2019. %G vs 4G: what is the difference. Viitattu 05.02.2021. https://www.raconteur.net/technology/5g/4g-vs-5g-mobile-technology/

Verizon. 2019. What is the different between 3G, 4G, 5G? viitattu 04.03.2021. https://www.verizon.com/about/our-company/5g/difference-between-3g-4g-5g

Woodford, C. 2020. Bluetooth. Viitattu 03.03.2021. https://www.explainthatstuff.com/howbluetoothworks.html

Zeus Integrated. 2019. A Brief History of Smart Home Automation. Viitattu 27.03.2021. https://zeusintegrated.com/blog/item/a-brief-history-of-smart-home-automation