Aleksi Martikainen ja Rasmus Suni

Älykotien IoT-laitteiden haavoittuvuudet ja hyökkäysvektorit

Tekniikan ja innovaatiojohtamisen
akateeminen yksikkö
Tekniikan kandidaatintutkielma
Automaatio ja tietotekniikka

Vaasa 2025

VAASAN YLIOPISTO
Tekniikan ja innovaatiojohtamisen akateeminen yksikkö
Tekijät: Aleksi Martikainen ja Rasmus Suni
Tutkielman nimi: Älykotien IoT-laitteiden haavoittuvuudet ja hyökkäysvektorit
Tutkinto: Tekniikan kandidaatintutkielma
Oppiaine: Automaatio ja tietotekniikka
Työn ohjaaja: Janne Koljonen
Valmistumisvuosi: 2025 **Sivumäärä:** **40**

TIIVISTELMÄ:
Esineiden internetin (IoT) nopea kehitys ja älykotien yleistyminen ovat parantaneet kotien toiminnallisuutta, energiatehokkuutta ja asumismukavuutta. Älykotien sovelluksien avulla pystytään kontrolloimaan ja automatisoimaan esimerkiksi kodin turvajärjestelmiä ja muita laitteita. Samalla teknologinen kehitys on kuitenkin lisännyt kyberturvallisuuteen liittyviä haasteita. Nämä uhat ja haasteet ovat merkittäviä riskitekijöitä käyttäjien sekä yhteiskunnan turvallisuudelle. Tässä kandidaatintutkielmassa tunnistetaan ja analysoidaan älykotien IoT-laitteisiin kohdistuvia hyökkäysvektoreita sekä tarkastellaan erilaisia suojautumismenetelmiä niiden torjumiseksi.

Tutkielman tavoitteena on selvittää, mitkä ovat älykotien IoT-laitteiden yleisimmät kyberturvahaavoittuvuudet ja hyökkäysvektorit sekä arvioida nykyisiä suojautumismenetelmiä älykotien tietoturvan parantamiseksi. Tutkielma on toteutettu kirjallisuuskatsauksena, jossa on hyödynnetty akateemisia artikkeleita ja tutkimuksia aiheesta. Keskeisiksi haavoittuvuuksiksi on havaittu käyttäjien puutteellinen tietoturvaosaaminen, laitteiden riittämätön suojaus ja teknologinen heterogeenisyys. Tutkielman lopuksi lukijalle esitetään suosituksia suojata oma älykotiympäristö konkreettisilla toimilla.

Tutkielmassa kerrataan IoT-laitteiden ja älykotien määritelmät. Lisäksi siinä perehdytään älykotien rakenteeseen, ominaisuuksiin ja erilaisiin sovelluksiin. Tutkielmassa tarkastellaan yleisimpiä hyökkäystyyppejä, kuten palvelunestohyökkäyksiä, salakuuntelu- ja tiedusteluhyökkäyksiä, välimieshyökkäyksiä, tietojenkalastelua ja huijaushyökkäyksiä, haittaohjelmia, signaalinhäirintää sekä fyysisiä hyökkäyksiä. Näistä erityisesti palvelunestohyökkäykset on osoittautuneet vakaviksi uhiksi. Tutkielmassa analysoidaan myös tunnettuja hyökkäystapauksia, kuten Mirai- ja BrickerBot-hyökkäyksiä, ja niiden vaikutuksia älykoteihin.

Älykotien keskeisiä suojautumismenetelmiä ovat esimerkiksi vahvat ja yksilölliset salasanat, monivaiheinen tunnistautuminen, tietoliikenteen salaustekniikat, ohjelmistojen säännöllinen päivittäminen, palomuurit sekä fyysiset suojaustoimet, kuten valvontakamerat. Tutkielmassa painotetaan myös käyttäjien tietoturvaosaamisen merkitystä ja kokonaisvaltaista riskienhallintaa. Tutkielman johtopäätöksinä todetaan, että IoT-laitteiden turvallisuuden parantaminen vaatii teknisiä ratkaisuja ja käyttäjien tietoisuuden lisäämistä. Tulevaisuuden kehityssuuntana on havaittu tekoälyn sekä koneoppimisen hyödyntämistä uhkien torjunnassa, biometrisiä tunnistautumismenetelmiä ja tiukempia kansainvälisiä tietoturvastandardeja.

AVAINSANAT: Haittaohjelma, Hyökkäysvektori, IoT, Kyberturvallisuus, Älykoti

Sisällys

Kuvat

Kuviot

Taulukot

Lyhenteet

DDoS	Distributed Denial of Service, Hajautettu estohyökkäys
DoS	Denial of Service, Estohyökkäys
MITM	Man-in-the-Middle, Välimieshyökkäys
IoT	Internet of Things, Esineiden internet
PDoS	Permanent Denial of service, Pysyvä estohyökkäys
VPN	Virtual Private Network, Virtuaalinen yksityisverkko
Wi-Fi	Wireless Fidelity, Langaton lähiverkko

1 Johdanto

Esineiden internetin (engl. Internet of Things, IoT) nopea kehitys on mullistanut useita elämänalueita monella eri tavalla, mutta erityisesti kotiemme teknologista infrastruktuuria. Älykotien järjestelmät mahdollistavat esimerkiksi lämmityksen, valaistuksen ja kodin eri turvallisuusratkaisujen hallinnan etäyhteyksien kautta. Älykodit, joissa useat IoT-laitteet ovat yhteyksissä toisiinsa ja internettiin, tarjoavat meille mukavuutta, energiatehokkuutta ja automaatiota (Lindsay ja muut, 2016, s. 1). Tämä tutkielma keskittyy tarkastelemaan älykotien IoT-laitteiden haavoittuvuuksia ja niihin liittyviä hyökkäysvektoreita. Lisäksi tutkielmassa tarkastellaan älykodin suojausmenetelmiä, jotka nousevat tutkimuksissa esille.

Älykotien yleistyminen on nostanut niiden kyberturvallisuuden keskeiseksi huolenaiheeksi. IoT-laitteiden haavoittuvuudet voivat tarjota ulkopuolisille mahdollisuuden tunkeutua kotiverkkoon ja kodin laitteisiin. Tällaiset tietoturvaloukkaukset voivat johtaa vakaviin yksityisyyden suojan rikkomuksiin sekä älylaitteiden haltuunottoon, mikä puolestaan mahdollistaa käyttäjien seuraamisen ja valvonnan älykotiympäristössä (Ali & Awad, 2018, s. 4). Yksi uhkaava esimerkki löytyy Pohjois-Amerikasta, jossa ulkopuolinen oli murtautunut perheen vauvamonitoriin ja ottanut laitteen hallintaansa. Hän oli huutanut yöllä perheen vauvalle ja käskenyt heräämään vauvamonitorin kaiuttimen kautta. Tämä törkeä yksityisyyden loukkaus, joka johtui IoT-laitteen kaappauksesta, on varoittava tapaus mahdollisista uhkatilanteista, joita älykodeissa voi ilmetä (Christie, 2014). Tällaiset tapaukset korostavat tarvetta tutkia ja kehittää älykotien kyberturvallisuutta.

1.1 Tutkielman tavoitteet ja tutkimuskysymykset

Tämän kandidaatintutkielman tavoitteena on tunnistaa ja analysoida, millaisia uhkia IoT-laitteisiin kohdistuu ja millä tavoin näitä uhkia voidaan torjua älykotiympäristössä. Tavoitteena on myös tarjota suosituksia, joiden avulla älykotien kyberturvallisuutta

voidaan parantaa ja kuinka suojata omia IoT-laitteita konkreettisilla toimilla. Tutkielman pyrkimyksenä on myös lisätä tietoisuutta yleisestä tietoturvallisuudesta kyberturvallisuuden ohella.

Tutkimuskysymyksinä tutkielmassa ovat:

1. Mitkä ovat älykotien IoT-laitteiden yleisimmät kyberturvahaavoittuvuudet?
2. Mitkä ovat älykoteihin kohdistuvat hyökkäysvektorit?
3. Miten nykyisiä suojautumismenetelmiä voidaan soveltaa älykotien kyberturvan parantamiseksi?

Näihin kysymyksiin vastaamalla pyritään syventämään ymmärrystä älykotien tietoturvaongelmista ja niiden ratkaisuista. Tämä tutkielma toteutetaan kirjallisuuskatsauksena, jossa analysoidaan aihetta käsitteleviä akateemisia artikkeleita ja tutkimuksia. Lähdemateriaali tutkielmaan haettiin useista tieteellisistä tietokannoista, kuten IEEE Xplore ja ScienceDirect. Materiaalin haussa käytettiin keskeisiä termejä, jotka liittyvät esineiden internettiin, digitaaliseen turvallisuuteen ja älykkäisiin asumisratkaisuihin. Lisäksi tutkielman lopussa esitetyt suositukset pohjautuvat tutkitun datan ja tilastojen avulla tehtyihin johtopäätöksiin. Tutkielmassa tuodaan esille tilastoissa korostuvia haavoittuvuuksia ja niiden kautta pyritään esittämään ennalta ehkäiseviä toimia.

1.2 Tutkielman rakenne

Tutkielma on jaettu useaan päälukukuun, joista kukin keskittyy eri osa-alueeseen älykotien kyberturvallisuudessa. Toinen luku kattaa yleiskatsauksen IoT-tekniikkaan ja älykotien rakenteeseen. Siinä käsitellään IoT-laitteiden määritelmää ja älykotien keskeisimpiä komponentteja ja sovelluksia. Kolmas luku esittelee älykotien IoT-laitteiden yleisimpiä haavoittuvuuksia ja niihin liittyviä hyökkäysvektoreita. Lisäksi luku käsittelee tunnettuja hyökkäystapauksia ja niiden vaikutuksia. Luvussa neljä keskitytään eri

suojausmenetelmien arviointiin ja riskienhallintaan. Luvussa pohditaan myös tulevaisuuden kehityssuuntia, älykoteihin kohdistuvien riskien tunnistamista ja eräässä tutkimuksessa tehtyä analyysia. Viides luku kokoaa yhteen tutkielman keskeiset tulokset ja esittää johtopäätökset. Lisäksi luvussa esitetään suosituksia älykotien kyberturvallisuuden parantamiseksi ja tarkastellaan aiheeseen liittyviä mahdollisia jatkotutkimuskohteita.

2 IoT ja älykodit

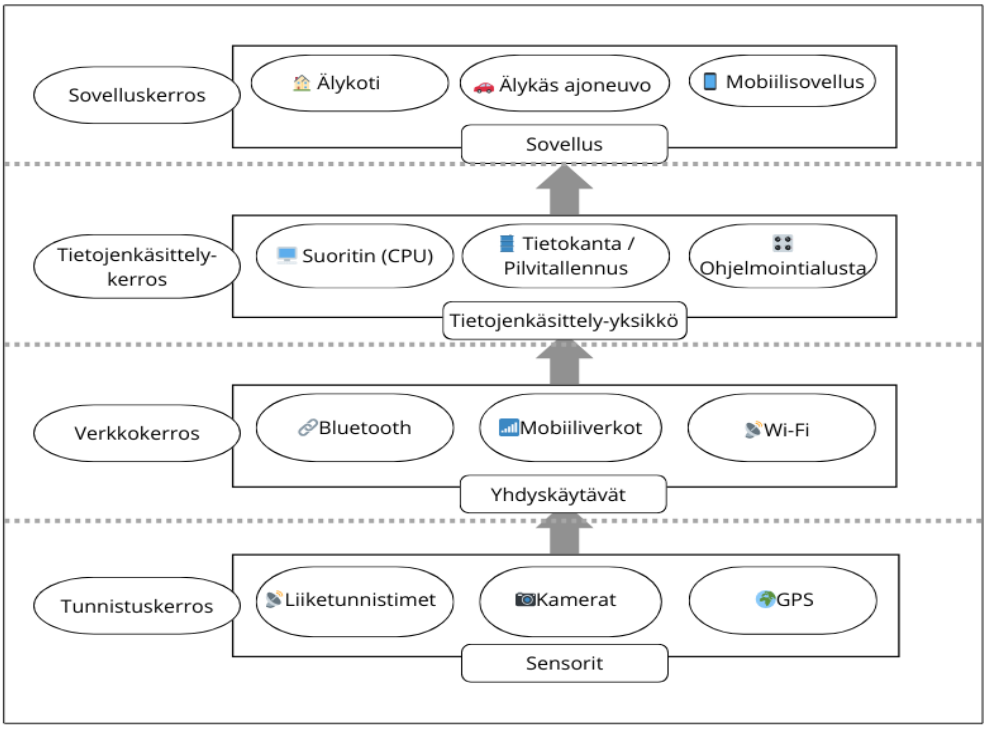
Tässä luvussa käsitellään IoT:n ja älykodin käsitteitä. Älykotien määrä on kasvanut merkittävästi viime vuosina. Niiden lukumäärä on lähestymässä 500 miljoonaa vuonna 2025. (Statista Research Department, 2025). Älykotien nopea kehitys viime vuosina on vaikuttanut arjen mukavuuksiin, mutta myös turvallisuusratkaisuihin. Tämä on nostanut esille uuden haasteen, jossa kodin turvallisuus ja yksityisyys ovat entistäkin haavoittuvammassa asemassa (Plachkinova ja muut, 2016, s. 1–2). Tämä on herättänyt paljon keskustelua maailmanlaajuisesti asian vakavuudesta. Älykodit koostuvat verkkoon liitetyistä laitteista (IoT), kuten lämmityksen, valaistuksen, turvajärjestelmien ja kodinkoneiden hallintajärjestelmistä, joita voidaan ohjata etäyhteyksien kautta. Laitteiden tarkoituksena on parantaa asumismukavuutta, energiatehokkuutta ja turvallisuutta (Hammi ja muut, 2022, s. 3). Seuraavissa kappaleissa tarkastellaan tarkemmin IoT-käsitettä sekä älykotien teknistä rakennetta ja sovelluksia.

2.1 Esineiden internet

Esineiden internet (engl. Internet of Things, IoT) viittaa fyysisten laitteiden, kuten ajoneuvojen, kodinkoneiden ja muiden esineiden verkostoihin, jotka on varustettu elektroniikalla, ohjelmistoilla, sensoreilla ja verkkoyhteydellä. Nämä ominaisuudet mahdollistavat näiden esineiden kerätä ja vastaanottaa dataa (Estrada ja muut, 2020 s. 82). Älykotien IoT-laitteet kommunikoivat keskenään käyttäen useita protokollia, kuten Wi-Fi, Bluetooth ja Zigbee (Aldahmani ja muut, 2023, s. 281). IoT:n perusajatuksena on luoda ympäristö, jossa laitteet toimivat automaattisesti yhtenäisenä kokonaisuutena, mikä tekee siitä älykkäämmän ja responsiivisemman (Gazis, 2021, s. 3).

IoT-laitteet yleistyvät jatkuvasti ja niiden määrä kasvaa eksponentiaalista vauhtia. Maailmassa on arvioitu olevan noin 18 miljardia IoT-laitetta, ja vuoteen 2030 mennessä tämän luvun odotetaan kasvavan jopa reiluun 32 miljardiin (Vailshery, 2024). IoT-laitteiden ominaisuudet vaihtelevat riippuen tyypistä, mallista, laitevalmistajasta sekä

tarkoitusperästä. Näiden laitteiden arkkitehtuuri koostuu tyypillisesti neljästä kerroksesta: tunnistus-, verkko-, tietojenkäsittely- ja sovelluskerroksesta (ks. kuva 1) (Sikder ja muut, 2018, s. 3–4).



Kuva 1. IoT-laitteiden arkkitehtuurikerrokset ja komponentit (mukaelma lähteestä Sikder ja muut, 2018, s. 3).

Jokainen kerros suorittaa oman tehtävänsä datan siirrossa ja käsittelyssä. Tästä hyvänä esimerkkinä voidaan pitää älykästä valvontajärjestelmää, joka toimii liiketunnistimella. Liiketunnistimen sensorit ja kamerat muodostavat järjestelmän ensimmäisen kerroksen eli tunnistuskerroksen, joka havainnoi ympäristössä tapahtuvat muutokset. Tämän jälkeen data, kuten video- ja kuvamateriaali siirtyy toiseen kerrokseen eli verkkokerrokseen, joka voi olla kyseisen laitevalmistajan oma palvelin. Data siirtyy seuraavaksi tietojenkäsittelykerrokseen analysoitavaksi, joka on kolmas vaihe prosessia. Tällä tasolla dataa käsitellään haluttuun muotoon, esimerkiksi luomalla kuvakollaasi pihatielle saapuvasta ajoneuvosta. Lopuksi sovelluskerros on vuorovaikutuksessa itse käyttäjän kanssa. Viimeinen taso tuottaa visuaalisen tuloksen IoT-laitteen lopulliseen

rajapintaan luomalla valmiin kokonaisuuden. Tämä näkyy esimerkiksi puhelimeen tulevana ilmoituksena, joka kertoo vieraan saapuneen kodin pihatielle.

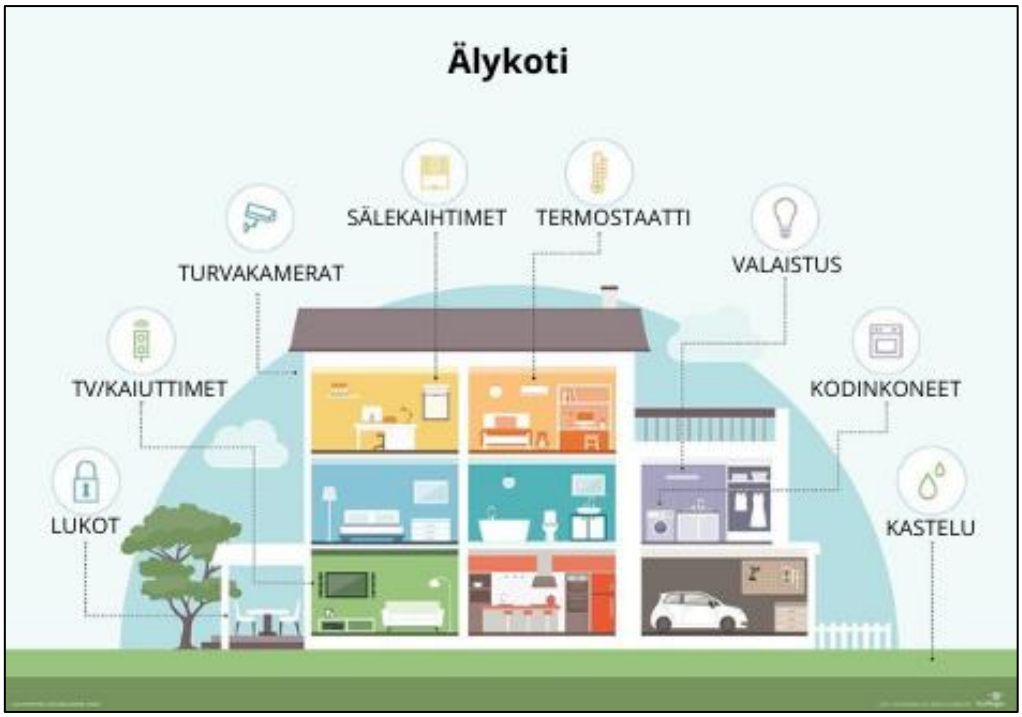
2.2 Älykodin määritelmä ja rakenne

Teknisestä näkökulmasta tarkasteltuna älykodilla tarkoitetaan asumismuotoa, jossa talon järjestelmät ja erilaiset laitteet on yhdistetty toisiinsa internetin välityksellä. Näin mahdollistetaan asuinympäristön etävalvonta, -hallinta ja -ohjaus (Ali & Awad, 2018, s. 2). Älykodin määritelmä vaihtelee kuitenkin tekijästä ja vuodesta riippuen. Sovacool ja Furszyfer Del Rio ovat koonneet taulukoihinsa asiantuntijoiden ja tutkijoiden kirjoittamia määritelmiä (2020, s. 5 ja s. 17). Tässä tutkielmassa älykodilla tarkoitetaan ympäristöä, jossa IoT-laitteisiin yhdistetty tietoliikenneverkko mahdollistaa niiden etäohjauksen, valvonnan tai hallinnan.

Älykoti eroaa tavallisesta kodista sen teknologisen edistyneisyytensä ansiosta. Siinä laitteet ovat kehitetty toimimaan automaattisesti tai jopa autonomisesti ilman käyttäjän jatkuvaa ohjausta. Usein avaintekijänä on laitteiden välinen yhteys, jonka avulla ne kommunikoivat keskenään (Barnes, 2020). Tämän vuoksi älykoteja mainostetaan usein moderneina, tehokkaina, asumismukavina ja turvallisina. Älykodeissa hyödynnetään paljon järjestelmiä ja laitteita, jotka palvelevat asukkaiden tarpeita. Osa älykodeista keskittyy erityisesti energiatehokkuuteen esimerkiksi hyödyntämällä aurinkopaneeleita tuottamaan sähköä kodin tarpeisiin. Toiset älykotien ratkaisut pyrkivät tukemaan asumismukavuutta ja kodin automaattista ohjausta. Esimerkiksi kodin laitteet ja järjestelmät ovat ohjattu helpottamaan arjen kotitöitä ja muita tehtäviä. Huolimatta älykotien erilaisista toteutustavoista, niitä yhdistävät IoT-laitteet ja tehokkuutta lisäävät ratkaisut (Abdullah ja muut, 2019, s. 139).

2.3 Älykotien keskeiset sovellukset

Kuten aiemmin on mainittu, IoT-laitteiden avulla pyritään automatisoimaan monia arkisia toimintoja ja tarjoamaan kattavampia valvonta- ja hallintamahdollisuuksia. Tässä kappaleessa käsitellään älykotien keskeisimpiä IoT-pohjaisia ratkaisuja ja tarkastellaan niiden tarjoamia ominaisuuksia. Kuvassa 2 esitetään älykotien keskeisiä ominaisuuksia.



Kuva 2. Älykodin keskeiset ominaisuudet (mukaelma lähteestä Yasar & Shea, 2023).

Keskeisimpiä sovelluksia älykodeissa ovat turvallisuus- ja valvontasovellukset. Älylukot mahdollistavat käyttäjille kulunvalvonnan ja ovien avauksen mobiilisovellusten kautta. Käyttäjien on mahdollista luoda määräaikaisia koodeja esimerkiksi vieraille tai huoltohenkilöstölle, mikä lisää turvallisuuden ja hallinnan tunnetta kodin asukkaille (Ho ja muut, 2016, s. 462). Lisäksi valvontakamerat ja liiketunnistimet tarjoavat kodin reaaliaikaisen seurannan etäyhteyden avulla. IoT-pohjaiset palovaroittimet ja vesivuotohälyttimet voivat havaita savun, kaasuvuodon tai vesivahingon, ja lähettää niistä hälytyksen suoraan käyttäjän mobiililaitteeseen. Tämä parantaa reagointinopeutta mahdollisissa hätätilanteissa (Kumar ja muut, 2016, s. 93). Nämä laitteet ovat erittäin

hyödyllisiä esimerkiksi kerrostaloissa, joissa asuu paljon asukkaita pienellä alueella. Lisäksi kerrostalojen ilmoitustaulut ovat tehty älykkäiksi niiden ominaisuuksillansa. Taulut ovat usein ohjelmoitu näyttämään esimerkiksi ajankohtaisia säätiedotteita tai muuta käyttäjille hyödyllistä informaatiota.

Automaattiset lämmitys-, ilmanvaihto- ja valaistusjärjestelmät ovat myös yleistyneet älykodeissa. Nämä tuovat huomattavaa asumismukavuutta ja ovat samalla järkeviä energiankulutusratkaisuja (Zhou ja muut, 2016, s. 37). Älykodeissa esimerkiksi valaistus voidaan asettaa reaktiiviseksi, jolloin huoneesta poistuttaessa valaistus himmenee tai sammuu automaattisesti sähkön säästämiseksi. Iso osa älykotien sovelluksista koostuu IoT-pohjaisista energianhallinta- ja tuotantojärjestelmistä. Optimaalinen tilanne olisi, että älykoti tuottaa oman energiamääränsä uusiutuvalla energialla, jonka se sitten kuluttaa. Esimerkiksi kodin lämmitysjärjestelmä on todettu toimivaksi tuomalla maalämpöratkaisut osaksi kodin lämpöverkkoa (Zhou ja muut, 2016, s. 31). Lisäksi aurinkopaneeliratkaisut ja muut energiantuotantojärjestelmät ovat keskeisiä osia älykodeissa, sillä ne mahdollistavat energiankulutuksen optimoinnin ympäristöystävällisiin ajankohtiin. Esimerkiksi aurinkopaneelit hyödyntävät auringon säteilyä silloin, kun tuotanto on korkeimmillaan. Tämä menetelmä vähentää kodin energiariippuvuutta verkosta ja pienentää myös samalla hiilijalanjälkeä (Kofler ja muut, 2012, s. 169).

Keskenään yhteydessä olevat kodinkoneet ja viihdejärjestelmät ovat lisäksi tuoneet lisää ulottuvuutta älykotien suunnittelussa. Esimerkiksi kodin älykkäät kontrollointijärjestelmät kuten Amazon Alexa, HomeKit ja Google Home toimivat useassa kodissa IoT-pohjaisina hallintajärjestelminä. Älykaiuttimina tunnetut Amazon Alexa -järjestelmät ovat keränneet suosiota, ja niitä on jo yli 600 miljoonaa kappaletta maailmassa (Panay, 2025). Sovelluksen tarkoituksena on koota älykodin erilaisia järjestelmiä yhteen, jolloin niitä voi hallita sanallisten komentojen avulla. Esimerkiksi kodin siivousjärjestelmä voi toimia robotti-imureilla, jotka siivoavat huoneistoa automaattisesti tai erillisillä ohjauskomennoilla. Nämä kaikki laitteet ovat yhdistetty

usein kodin sisäiseen internet-verkkoon langallisesti tai langattomasti. Laitteet luovat IoT-laiteverkon, joka toimii kodin keskitettynä hallintajärjestelmänä. Älykodeissa siis on loputtomasti mahdollisuuksia sovelluksille ja uudelle tekniikalle.

IoT-teknologian sovellukset laajenevat myös terveyden ja hyvinvoinnin alueelle. Esimerkiksi älypatjat seuraavat käyttäjän unenlaatua ja mukauttavat sängyn lämpötilaa parhaan mahdollisen unen takaamiseksi. Tällä tavalla ne voivat jopa havaita mahdollisen uniapnean nukkujalla (Sangeetha ja muut, 2022, s. 1). Tällaiset sovellukset edistävät terveellisiä elämäntapoja ja tukevat asumismukavuutta. Lisäksi elintarvikkeiden säilyttämiseen tarkoitetut jääkaappi ja pakastin voivat tulevaisuuden ratkaisuilla kertoa asukkaiden ruokavarantojen laatua ja määrää. Nämä kodinkoneet voisivat tilata lisää ruokaa Internet-kanavien välityksellä ja toimia itsenäisesti ilmoittaessaan jopa eräpäiväykset ja mahdolliset reseptiehdotukset talon asukkaille (Rouillard, 2013, s. 3).

3 IoT-laitteiden kyberturvallisuus ja haavoittuvuudet

Tässä luvussa keskitytään tarkastelemaan IoT-laitteiden kyberturvaa. Luvun tavoitteena on tarjota yleiskuva siitä, miksi kyberturvallisuus on keskeinen tekijä IoT-laitteiden käytössä, millaisia haavoittuvuuksia IoT-laitteisiin liittyy ja miten hyökkääjät voivat hyödyntää näitä haavoittuvuuksia erilaisin hyökkäysvektorein. Luvussa analysoidaan tunnettuja hyökkäystapauksia sekä arvioidaan niiden vaikutuksia älykotiympäristöissä.

3.1 Kyberturvallisuus haasteena älykotien IoT-infrastruktuurille

Älykotien suurin haavoittuvuus IoT-laitteissa on niiden käyttäjä itse (Arabo, 2015, s. 229). Ihminen tuo omalla käytöllänsä laitteisiin inhimillisiä tekijöitä, jotka avaavat mahdollisuudet haavoittuvuuksille. Ensimmäisenä haavoittuvuutena korostuu yleisen tietämyksen puute. Toisin sanoen käyttäjän on vaikeaa havaita mahdollisia uhkakuvia ja varautua niihin. Laitteen tai järjestelmän omistaminen ei välttämättä tarkoita ammattitaitoisuutta sen käyttämiseen. Tietojen ja taitojen puute voivat johtaa seuraavaan haavoittuvuuteen eli puutteelliseen suojaukseen IoT-laitteissa. Tämä ilmenee yleensä heikkoina salasanoina suojaamattomissa verkkoyhteyksissä tai puutteellisesti suunnittelulla ohjelmistoina (Hammi ja muut, 2022, s. 1–2). Kun IoT-laitteet linkittyvät yhtenäiseksi palveluverkoksi, haavoittuvuudet moninkertaistuvat, ja hyökkääjät voivat saada pääsyn koko järjestelmään (Abdullah ja muut., 2019, s. 142).

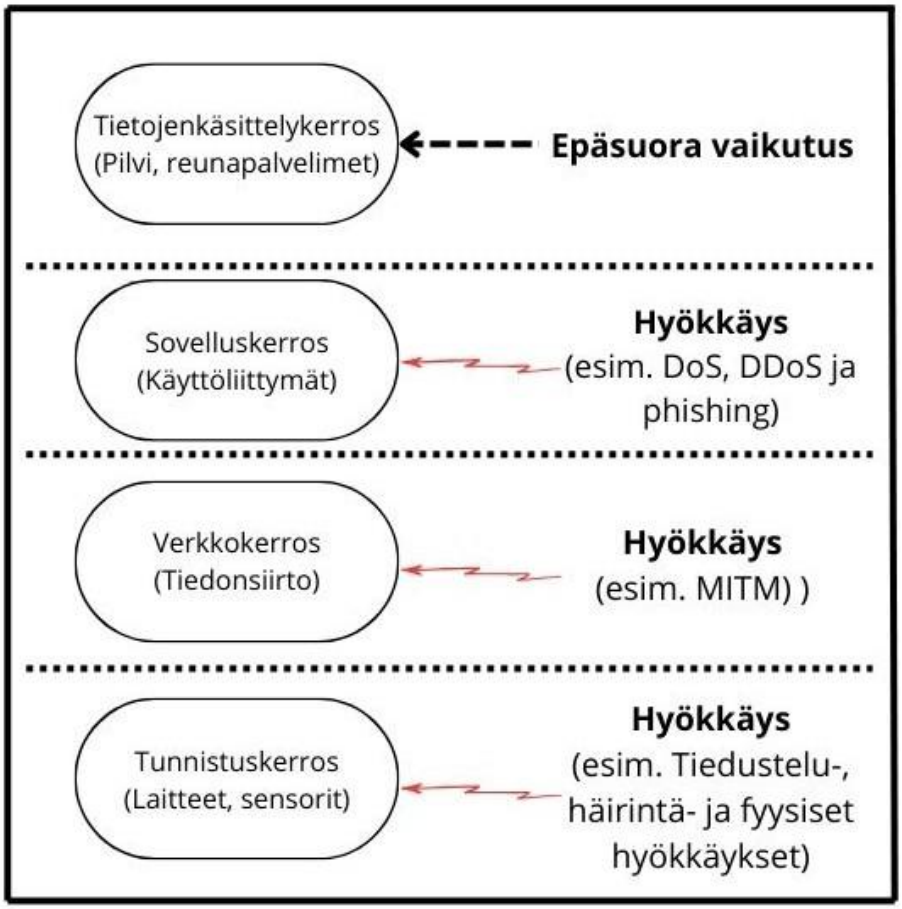
Kyberrikollisten vaatimat lunnasrahat ovat kasvussa, ja yhä useammat yritykset joutuvat maksamaan merkittäviä summia saadakseen takaisin hallintaansa menetetyn datan. Vuonna 2021 noin 11 prosenttia yhdysvaltalaisista yrityksistä maksoi yli miljoona dollaria hakkereille, kun taas pienempien, alle 10 000 dollarin lunnaita maksaneiden yritysten osuus putosi 34 prosentista 21 prosenttiin (Aldahmani ja muut, 2023, s. 2). Vaikka älykodit eivät teknisesti ja taloudellisesti ole yhtä houkuttelevia kohteita kuin suuret yritykset, niiden sisältämät henkilökohtaiset ja arkaluonteiset tiedot tekevät niiden suojelemisesta entistäkin tärkeämpää (Arabo, 2015, s. 229). Myös Aldahmani ja muut

(2023, s. 2) korostavat, että älykotien tietoturvariskit eivät rajoitu pelkästään taloudellisiin menetyksiin. Niillä voi myös olla vakavia yksityisyyden suojan seurauksia, kuten arkaluontoisten terveystietojen paljastuminen, mikä voi vaarantaa asukkaiden turvallisuuden.

Pelkkä yksittäisten ongelmien korjaaminen ei riitä, vaan kyberturvallisuuteen tarvitaan laajempi lähestymistapa, joka huomioi kaikki mahdolliset riskit. Tämä korostaa tarvetta parantaa sekä laitteiden suunnittelua että käyttäjien tietoisuutta turvallisuuden varmistamiseksi (Aldahmani ja muut, 2023). Estrada ja muut (2020, s. 81–82) painottavat, että on välttämätöntä ”lukita ovi” estääkseen tunkeilijat, mutta samalla on varmistettava, ettei jätä mitään ”ikkunoita auki”. Tämä metafora kuvastaa hyvin tarvetta kokonaisvaltaiselle lähestymistavalle IoT-laitteiden turvallisuuden varmistamisessa.

3.2 Yleisimmät hyökkäystyypit ja niiden vaikutukset älykodeissa

Älykodin joutuessa hyökkäyksen kohteeksi, voi olla vaikeaa tunnistaa kotiin kohdistuvan hyökkäyksen laatu. Hyökkäykset kohdistuvat yleensä kolmeen eri kerrokseen. IoT-arkkitehtuuri koostuu neljästä kerroksesta (ks. kuva 1), mutta hyökkäykset kohdistuvat yleensä vain tunnistus-, verkko- ja sovelluskerrokseen. Tietojenkäsittelykerros on läheisesti sidoksissa verkko- ja sovelluskerrosten kanssa, joten se yhdistetään usein näihin kerroksiin kuvan 3 mukaisesti. Rikoslain (laki tieto- ja viestintärikoksista 578/1995) mukaan pahimmassa tapauksessa puhutaan hyvin vakavista rikosnimikkeistä, jos mukana on laitteiden häiritsemistä, kaappaamista tai manipulointia. Tällaiset rikokset voivat johtaa asukkaiden taloudelliseen kiristämiseen ja ohjaamaan muihin pakkokeinojen käyttöön. Hyökkääjät voivat myös hyödyntää heikosti suojattuja IoT-laitteita liittämällä ne osaksi botnet-verkkoja, joiden avulla voidaan toteuttaa laajamittaisia hyökkäyksiä. Tunnettuja esimerkkejä tällaisista hyökkäyksistä ja niiden seurauksia käsitellään tarkemmin alaluvussa 3.3.



Kuva 3. IoT-laitteiden arkkitehtuurikerrokset.

3.2.1 Palvelunestohyökkäykset

Palvelunestohyökkäykset (engl. Denial of service, DoS) ja hajautetut palvelunestohyökkäykset (engl. Distributed Denial of Service, DDoS) ovat hyökkäyksiä, joiden tarkoituksena on häiritä älykotien IoT-infrastruktuurin toimintaa (Huraj ja muut, 2020). Palvelunestohyökkäyksessä kohdelaitetta tai palvelua pyritään ylikuormittamaan haitallisella verkkoliikenteellä niin, ettei se kykene käsittelemään oikeiden käyttäjien lähettämiä pyyntöjä (Neshenko ja muut, 2019, s. 14; Touqeer ja muut, 2021 s. 14071). Älykodin IoT-järjestelmissä hyökkääjä voisi lähettää suuren määrän dataa kohteena olevalle laitteelle. Esimerkiksi älykotien keskitetyn ohjausjärjestelmän kuormittaminen voisi estää asukkaita säätämästä valaistusta, lämmitystä tai turvajärjestelmiä. Hajautetussa palvelunestohyökkäyksessä haitallinen liikenne ohjataan kohteeseen

useasta eri lähteestä samanaikaisesti. IoT-laitteet ovat alttiita tällaisille hyökkäyksille, koska niiden tietoturva on usein puutteellisesti toteutettu (Huraj ja muut, 2020, s. 1).

3.2.2 Tiedusteluhyökkäykset ja salakuuntelu

Tiedusteluhyökkäykset ja salakuuntelu (engl. eavesdropping) kuuluvat tunnistuskerrokseen kohdistuviin hyökkäyksiin. Tässä ulkopuolinen taho tai henkilö pyrkii seuraamaan ja kuuntelemaan käyttäjän toimintaa ja liikkuvaa informaatiodataa (Xia & Brustoloni, 2005, s. 490). Hyökkäys liitetään yleensä tiedusteluun ja salakuunteluun, koska nämä tapahtuvat käyttäjän tiedostamatta ja ilman hänen suostumustaan. Tässä hyökkääjä rikkoo käyttäjän yksityisyyttä ja saa haltuunsa arkaluontoista tietoa, esimerkiksi pankkitunnuksia tai muuta kriittistä dataa. Tämä tapahtuu seuraamalla uhrin lähettämää ja vastaanottamaa dataliikennettä. IoT-laitteet, jotka jäävät heikolle huomioinnille voivat olla riskikohteena tiedusteluhyökkäyksiin (Touqeer ja muut, 2021 s. 14070). Älykotiympäristössä lähes jokainen IoT-laite on haavoittuva salakuuntelulle, koska niiden ominaisuuksiin kuuluvat mikrofoni- ja kuuntelujärjestelmät.

3.2.3 Välimieshyökkäykset

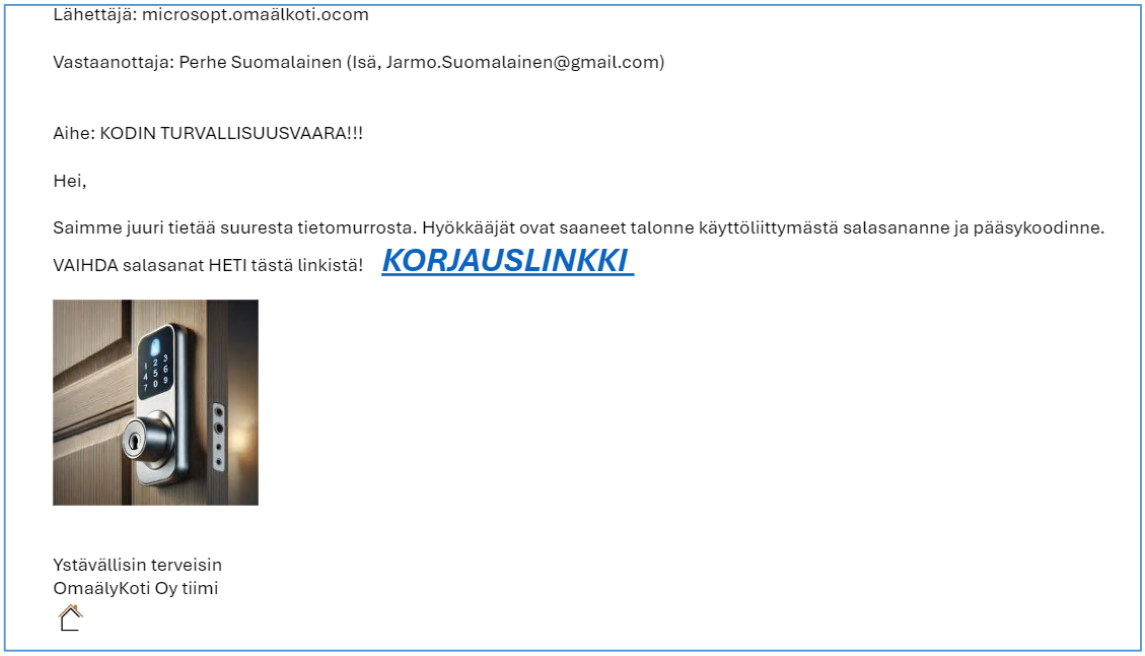
Välimieshyökkäys (engl. Man-in-the-Middle, MITM) kuuluu verkkokerrokseen kohdistuviin hyökkäyksiin. Välimieshyökkäyksessä hyökkääjä tunkeutuu salaa kahden osapuolen, kuten käyttäjän ja laitteen väliseen viestintään (Almahdami ja muut, 2023, s. 7). Tämän avulla hyökkääjä voi salakuunnella ja manipuloida tietoliikennettä osapuolten välillä (Mallik, 2018, s. 113). Tunkeutuja häiritsee yhteyttä hyödyntäen IoT-laitteiden toimintaperiaatteita, esimerkiksi langatonta tiedonsiirtoa ja niiden heikkoja suojaustasoja. Sen jälkeen hyökkääjä varastaa mahdollisesti arkaluontoisia tietoja ja tunnuksia samalla, kun käyttäjä ja palvelin yrittävät kommunikoida (Touqeer ja muut, 2021 s. 14072).

Välimieshyökkäykset voivat olla erityisen vaikeasti havaittavissa, mikäli hyökkäyksen toteuttaja on ammattimainen ja käyttää kehittyneitä tekniikoita dataliikenteen kaappaamiseen ja manipulointiin (Mallik, 2018, s. 113). On kuitenkin mahdollista, että ennen välimieshyökkäystä, tunkeutuja on pyrkinyt tiedustelemaan ja salakuuntelemaan käyttäjän toimintaa, jotta hänellä olisi ennakkotietoa hänen käyttäytymisestään. Suojaamattomat reitittimet ja langattomat verkot ovat alttiita välimieshyökkäyksiin älykodeissa. Näiden verkkoliikenne suojaamattomana on erittäin haavoittuvainen.

3.2.4 Huijaus- ja tietojenkalasteluhyökkäykset

Huijaus- ja tietojenkalasteluhyökkäykset (engl. spoofing, phishing) ovat sovelluskerrokseen kohdistuvia hyökkäyksiä. Huijaamis-, väärentämis- ja kalasteluhyökkäyksinä tunnetut hyökkäykset ovat olleet erittäin yleisiä viime vuosina. Maailmanlaajuisesti kalasteluviestejä lähetetään sähköpostitse 3,4 miljardia päivittäin (Griffiths, 2025). Näissä hyökkäyksissä hyökkääjä pyrkii esiintymään toisena henkilönä, yrityksenä, palveluna tai verkko-osoitteena väärennettyjen tietojen avulla. Tavoitteena on saada kohde luottamaan väärennökseen ja sitä kautta paljastamaan tietoja, kuten salasanoja tai pankkitietoja (Nirmal ja muut, 2020, s. 2327).

Sähköpostiviestit kiireellisestä asiasta ovat tyypillisiä esimerkkejä kalasteluyrityksestä (Gupta ja muut, 2016, s. 3632). Viesti sisältää yleensä linkin tai toimintakehotteen, jonka kautta hyökkääjä pyrkii saamaan yhteyden kohteeseensa, kuten kuvan 4 esimerkissä havainnoidaan. Käyttäjä luottaa hyökkääjän luomaan väärennökseen ja jakaa vapaaehtoisesti omat arkaluonteiset tiedot eteenpäin. Nämä huijaukset ovat petollisia niiden häikäilemättömyyden, aitouden ja yleisyyden takia. Epäilyttävä linkki voi koitua kalliiksi taloudellisesti ja tietoturvallisuuden kannalta, mikäli linkin kautta ladattu tiedosto sisältää haittaohjelman, joka leviää koko järjestelmään (Gupta ja muut, 2016, s. 3632).



Kuva 4. Esimerkki sähköpostikalastelusta älykodin omistajalle.

3.2.5 Haittaohjelmahyökkäykset

Haittaohjelmat (engl. malware) muodostavat merkittävän turvallisuusriskin älykotien IoT-järjestelmissä. Haittaohjelmien tavoitteena on päästä laitteeseen tai järjestelmään luvattomasti, häiritä niiden toimintaa tai varastaa arkaluontoista dataa käyttäjiltä (Alshamsi ja muut, 2024, s.10). Haittaohjelmiksi luokitellaan monenlaiset vahingolliset ohjelmat, kuten virukset, madot, troijalaiset, kiristyshaittaohjelmat, vakoiluohjelmat ja botnet-ohjelmat (Alshamsi ja muut, 2024, s. 3). Näistä botnet-ohjelmat ovat erityisen vaarallisia IoT-laitteile. Niiden avulla hyökkääjä voi hallita useita laitteita samanaikaisesti ja hyödyntää niitä laajempiin hyökkäyksiin, kuten hajautettuihin palvelunestohyökkäyksiin (Angrishi, 2017, s. 4). Haittaohjelmat voivat päästä IoT-laitteisiin erityisesti heikosti suojattujen verkkorajapintojen, heikkojen salasanojen tai ohjelmistojen tietoturvahaavoittuvuuksien kautta. Lisäksi laitteiden rajoitetut laskentaresurssit, pienet prosessorit ja vähäinen muisti tekevät niiden suojaamisesta tavanomaisilla kyberturvaratkaisuilla haastavaa, mikä edelleen lisää haittaohjelmien uhkaa IoT-laitteisiin (Khan ja muut, 2018, s. 3; Rao & Haq, 2018, s. 34).

3.2.6 Häirintähyökkäykset

Häirintähyökkäys eli signaalin häirintä (engl. jamming) on yleinen tunnistuskerroksen hyökkäystapa. Cyber-Reconin (2020) mukaan langattoman viestinnän häirintähyökkäykset voidaan jakaa kahteen päätyyppiin: reaktiiviseen ja jatkuvaan häirintään. Reaktiivinen häirintä toteutetaan ainoastaan silloin, kun laitteet yrittävät aktiivisesti kommunikoida keskenään. Tämän tarkoituksena on kohdistaa häiriö tarkasti tiettyihin viestintätilanteisiin ja vaikeuttaa näin järjestelmän normaalia toimintaa. Jatkuva häirintä puolestaan lähettää jatkuvasti häiriösignaalia, pyrkien katkaisemaan laitteiden välisen yhteyden kokonaan ja estämään kaiken viestinnän laitteiden välillä (Cyber-Recon, 2020).

Myös hyökkäykset voivat erota voimakkuudeltaan toisistaan, koska tarpeeksi vahvalla häirinnällä voidaan pyrkiä lamauttamaan kokonaan vallitseva systeemi (Touqeer ja muut, 2021 s. 14075). Hyökkäys siis estää käyttäjän toiminnan ”kuurouttamalla” IoT-laitteen viestintäyhteydet signaalihäirinnällä. Tämä voidaan toteuttaa vahvoilla taajuuslähettimillä vastaanottavaan laitteeseen. Etenkin langattomasti toimivat järjestelmät ovat haavoittuvaisia tälle hyökkäykselle (Touqeer ja muut, 2021 s. 14075). Tästä yksi esimerkki voisi olla älykodin lukitusjärjestelmän häiritseminen. Käyttäjä ei pääse enää kotiinsa sisälle, jos langatonta signaalia häiritään ja se tehdään toimintakyvyttömäksi.

3.2.7 Fyysiset hyökkäykset

Fyysinen haavoittuvuus on yksi tunnistuskerroksen keskeisistä ongelmista. Koska monet älykotilaitteet, kuten valvontakamerat, älylukot ja liiketunnistimet sijaitsevat ulkona, ne ovat alttiita manipulaatiolle, vahingoittamiselle tai varastamiselle (Aldahmani ja muut, 2023, s. 6). Hyökkääjä voi esimerkiksi asentaa väärennetyn sensorin, joka ohjaa kodin

tietoliikenteen hyökkääjän hallussa olevaan järjestelmään. Lisäksi laitteiden rikkominen ei vaadi suurta voimaa, koska laitteet voivat olla rakenteellisesti herkkiä. Myös erittäin kriittisenä osana IoT-laitekokonaisuuksia on niiden käyttövoima. Laitteet tarvitsevat erittäin paljon sähköä toimiakseen, niin virtalähteen katkaiseminen tai lamauttaminen saa laitteet toimintakyvyttömäksi (Touqeer ja muut, 2021 s. 14075). Tämä saattaa olla erityisen haitallista hälytysjärjestelmien tai elektronisten lukkojen kohdalla, sillä niiden vikaantuminen voi jättää asukkaat suojattomiksi fyysisiltä uhilta. Tunnistuskerroksen suojaaminen on näin ollen kriittistä älykotien turvallisuuden ja luotettavuuden kannalta.

3.3 Tunnetut hyökkäystapaukset ja niiden vaikutukset

Älykotien IoT-laitteet, kuten vauvamonitorit ja turvakamerat keräävät jatkuvasti arkaluontoista dataa ja ovat useasti heikosti suojattuja altistaen laitteet hyökkäyksille (Anand ja muut 2020, s. 168826). Näiden laitteiden tyypillisiä haavoittuvuuksia ovat esimerkiksi heikot salasanat, salaamattomat yhteydet sekä valmistajien vähäinen panostus kyberturvallisuuteen altistaen ne hyökkäyksille (Anand ja muut 2020, s. 168826; Hammi ja muut, 2022, s. 1–2). Tämä onkin viime vuosina johtanut siihen, että laajamuotoisia verkkohyökkäyksiä on tapahtunut.

Hyvänä esimerkkinä tästä voidaan pitää Mirai-nimistä verkkohyökkäystä, joka tapahtui vuonna 2016. Hyökkäyksen mahdollisti laitteiden heikko tietoturva, jota hyökkääjät käyttivät hyväkseen. Monet IoT-laitteet, kuten reitittimet ja digitaaliset videotallentimet olivat helposti hakkeroitavissa. Niissä tietoturvallisuutta vähensivät oletussalasanat palvelimissa, puutteelliset ohjelmistopäivitykset ja suojaamattomat verkkoyhteydet (Mahlous, 2022, s. 59). Heikkoa tietoturvaa hyödynnettiin haittaohjelmien asentamiseen laitteisiin. Tarttunut laite lopulta liitettiin hyökkääjien toimesta osaksi Mirai-botnettiä, joka pystyi vastaanottamaan komentoja hyökkääjiltä. Tätä käytettiin suorittamaan massiivinen määrä DDoS-hyökkäyksiä erilaisille palvelimille. Jokainen tartunnan saanut laite voitiin täten valjastaa hyökkääjien käyttöön. Pahimmillaan Mirai-hyökkäys sai

tartutettua arvioltaan 4000 IoT-laitetta tunnissa, mikä kuvaa sen tehokkuutta ja laajuutta (Angrishi, 2017, s. 6).

Lisäksi yksi tunnetuin, mutta samalla tuhoisin IoT-botneteistä on ollut tapaus nimeltä BrickerBot vuonna 2017. BrickerBotin tarkoituksena ei ollut IoT-laitteiden lamauttaminen vaan pyrkimyksenä oli tuhota ne kokonaan. Laitteisiin murtautumisen jälkeen BrickerBot suoritti PDoS-hyökkäyksen (engl. permanent denial-of-service), joka aiheutti laitteiden käyttökelvottomuuden pysyvästi (Abaimov, 2024, s. 330). Laitteita ei ollut enää mahdollista tämän jälkeen korjata ilman fyysistä palautusta. Tässäkin heikko IoT-laitteiden suojaus koitui näiden hyökkäyksien kohtaloksi. BrickerBot murtautui IoT-laitteiden järjestelmään väsytyshyökkäyksellä (engl. brute forcing), jonka jälkeen se loi pääsyn laitteen hallintajärjestelmään (Abaimov, 2024, s. 327).

Käytännön esimerkkinä älykotijärjestelmään kohdistuneesta DDoS-hyökkäyksestä löytyy myös Suomesta vuonna 2016, jossa kahden älyrakennuksen IoT-järjestelmät yrittivät automaattisesti torjua hyökkäystä. Tämän seurauksena lämmönjakelusta, ilmanvaihdosta ja lämminvesijärjestelmistä vastaavat laitteet joutuivat toistuvaan uudelleenkäynnistyskierteeseen ja estivät pääsyn etähallintaan. Kyseiset järjestelmät olivat toimintakyvyttömiä yli viikon ajan (Huraj ja muut, 2020, s. 3). Tämä Lappeenrannassa tapahtunut hyökkäys oli myös Mirai-botnettiin pohjautuva. Tapauksessa korostui älykotien tietoturvan laiminlyönti, sillä asuinrakennuksista puuttuivat keskeiset suojausratkaisut, kuten palomuuri, joka olisi voinut estää tai rajoittaa hyökkäyksen vaikutuksia (Angrishi, 2017, s. 10).

4 Suojautumismenetelmien arviointi ja riskienhallinta

Tässä luvussa arvioidaan erilaisia suojautumismenetelmiä liittyen IoT-laitteiden kyberturvallisuuteen älykotiympäristössä. Nämä suojautumismenetelmät sisältävät sekä käyttäjäkohtaisia että ulkoistettuja tapoja suojautua mahdollisilta uhkakuvilta. Lisäksi luvussa tunnistetaan ja kartoitetaan älykotien riskejä liittyen kyberturvallisuuteen. Potentiaalisten riskien kartoittaminen parantaa valmiutta varautua niihin. Lopuksi luvussa tarkastellaan älykotien kyberturvallisuuden tulevaisuuden kehityssuuntia ja uusia ratkaisuja, joiden avulla voidaan parantaa IoT-laitteiden turvallisuutta.

4.1 Riskien tunnistaminen ja arviointi älykodeissa

Älykotien IoT-järjestelmien turvallisuuden varmistaminen edellyttää mahdollisten riskien tunnistamista ja arviointia. Riskienhallinta alkaa riskien tunnistamisella, jossa arvioidaan mahdollisia uhkia, haavoittuvuuksia ja niihin liittyviä seurauksia. IoT-laitteiden monimutkaisuus, heterogeenisyys ja nopea kehitys vaikeuttavat kokonaiskuvan muodostamista, mikä tekee riskien tunnistamisesta haastavaa (Alrawi ja muut, 2019, s. 1362; Brass ja muut, 2018). Ajankohtaisien uutisten seuraaminen ja omien laitteiden tilan valvonta ovat keskeisiä tekijöitä riskien tunnistamisessa. Esimerkiksi Linnakkeen ja Kärkkäisen (2025) kirjoittama tietoturvauutinen kuvaa tarkasti oman kodin reitittimeen kohdistuvia vaaroja. Myös keskeisessä osassa älykotien turvallisuuden arvioinnissa ovat haavoittuvuusanalyysit ja riskimatriisit. Näissä kartoitetaan ja testataan älykotien ominaisuuksia torjua ja havaita mahdollisia uhkakuvia ja riskitilanteita (Kavallieratos ja muut, 2019). Analysoidessa älykotien turvallisuutta olisi hyvä ottaa huomioon sekä hyökkääjän, että uhrin näkökulma. Näillä keinoilla mahdolliset haavoittuvuudet tulevat ilmi, mutta myös riskien hallinta ja niihin varautuminen on helpompaa (Kavallieratos ja muut, 2019, s. 4).

4.2 Nykyiset suojautumismenetelmät älykodeissa

Älykotien suojausjärjestelmät ovat monitasoinen kokonaisuus, ja ne ovat kehittyneet paljon viime vuosina. Älykotien turvallisuustaso on keskeinen prioriteetti suunnitteluvaiheessa. Yleisimmät suojausmenetelmät voidaan jakaa tunnistus-, verkko- ja sovelluskerrokseen. Näiden menetelmien avulla pyritään minimoimaan haavoittuvuudet ja varmistamaan, että älykodin käyttäjät voivat hyödyntää teknologiaa turvallisesti ja luotettavasti.

Tunnistuskerroksen suojausmenetelmät keskittyvät pääosin fyysisiin suojautumismenetelmiin. Nämä otetaan jo suunnittelu- ja rakennusvaiheessa huomioon, koska älykodit pyritään rakentamaan tehokkaiksi ja turvallisiksi. Suojatusti rakentaminen pitää sisällään esimerkiksi valokuitukaapeleiden asennuksen maan alle ja talon pääsisäänkäyntien selkeän suunnittelun. Tämä estää laitteiden tai järjestelmien peukaloinnin ulkopuolelta (Touqeer ja muut, 2021 s. 14078). Sisäänkäynnit yleensä varustellaan valvonta- ja tunnistusjärjestelmillä, jotka voivat olla älykameroita ja liiketunnistimia. Jotkut järjestelmät myös integroidaan kodin lukitusjärjestelmään, jolloin ovet voidaan avata tunnistetiedoilla tai etäyhteydellä asukkaille (Ho ja muut, 2016, s. 463). Kodin suojausmenetelmiin kuuluu myös varautuminen ilkivaltaan ja varkauksiin. Näissä tilanteissa vakuutusyhtiöiden tarjoamat vakuutussopimukset, kattavat kodin laitteiden vahingoittumisen, ilkivallan tai varkaudet. Vakuutukset yleensä kattavat laitteiden korjaus- ja uusimiskulut. Lisäksi varavirtajärjestelmät voivat varmistaa tunnistuskerroksen laitteiden toimintavarmuuden sähkökatkojen aikana (Ouramdane ja muut, 2022). Esimerkiksi kodin energiariippuvuus voidaan korvata jaksollisesti akkuvarannoilla, etteivät älykodin turvajärjestelmät pettäisi.

Verkkokerroksen suojausmenetelmät koostuvat pääosin internet-yhteydellä toimiviin laitteisiin ja niiden muodostamiin kokonaisuuksiin. Verkkokerroksessa suojataan reitittimet, älylaitteet ja tiedonsiirto erilaisilta hyökkäyksiltä sekä haitalliselta liikenteeltä. Avoimien yhteyksien muuttaminen salattuihin ja suljettuihin yhteyksiin tehostaa langattomien verkkojen suojausta ja varmistaa pilvipalveluiden sekä älylaitteiden

tiedonsiirron. Esimerkiksi VPN-yhteys tai verkon segmentointi voi auttaa pitämään sisäisen Wi-Fi-yhteyden älylaitteiden sisällä (Abdullah ja muut, 2019, s. 144). Tämä estää hyökkääjän tunkeutumisen jokaiseen laitteeseen.

Myös reitittimien suojaaminen palomuureilla tai muilla virustorjuntaohjelmilla parantaa älykodin kyberturvallisuutta (Abdullah ja muut, 2019, s. 144). Tämä toimi voi rajoittaa ja havaita poikkeavaa verkkoliikennettä, mutta samalla estää hyökkääjän tunkeutumista järjestelmään. Vaikka sovellusten ja ohjelmistojen päivitykset ovat osa sovelluskerroksen suojautumismenetelmiä, ne ovat olennainen tekijä älykodin kyberturvallisuudessa. Ne parantavat myös verkkokerroksen suojautumista esimerkiksi estämällä haittaohjelmien leviämistä tai korjaamalla haavoittuvuuksia. Tämä mahdollistaa myös verkkokerroksen suojautumisen, jotta tunkeutuja ei pääse lataamaan haittaohjelmia kodin järjestelmiin (Abdullah ja muut, 2019, s. 144). Lisäksi WPA3-salaus, HTTPS-protokollan käyttäminen, MAC-osoitteiden suodatus tuovat lisää turvallisuutta verkkokerrokseen. Nämä suojautumismenetelmät estävät hyökkääjää muokkaamasta verkkoliikennettä, luvattomasti järjestelmiin pääsyä ja suojaavat IoT-laitteiden datansiirtoa.

Sovelluskerroksen suojautumismenetelmät keskittyvät käyttäjärajapinnan turvatoimiin, kuten henkilöllisyyden varmentamiseen, tietojen salaamiseen ja pääsynhallintaan. Ensimmäisenä suojautumismenetelmänä toimii käyttäjän henkilöllisyyden varmentaminen. Monivaiheisentunnistuksen (engl. multi-factor authentication, MFA) tarkoitus on varmistaa käyttäjän henkilöllisyys ja sallia pääsy vain oikealle henkilölle (Roman ja muut, 2013, s. 2271). Yleiset monivaihetunnistukset voidaan nykyään optimoida käyttäjän sormenjälkeen, kasvojen tunnistamiseen tai muuhun henkilökohtaiseen tietoon. Tunnistaminen liittyy hyvin paljon myös sovelluskerroksen salaamiseen. Tämä tarkoittaa vahvoja salausmenetelmiä salasanoilla tai komentojen suorittaminen kryptattuna. Ulkopuoliset käyttäjät eivät pääse käsiksi järjestelmään tai muihin arkaluontoisiin tietoihin järjestelmän sisällä. Jos tämä tapahtuu, niin salauksella varmistetaan, että tunkeutuja ei voi käyttää saamaansa dataa hyväksi (Touqeer ja muut, 2021 s. 14079). Myös lokiauditointi ja hälytysilmoituksien tarkka asettaminen ja

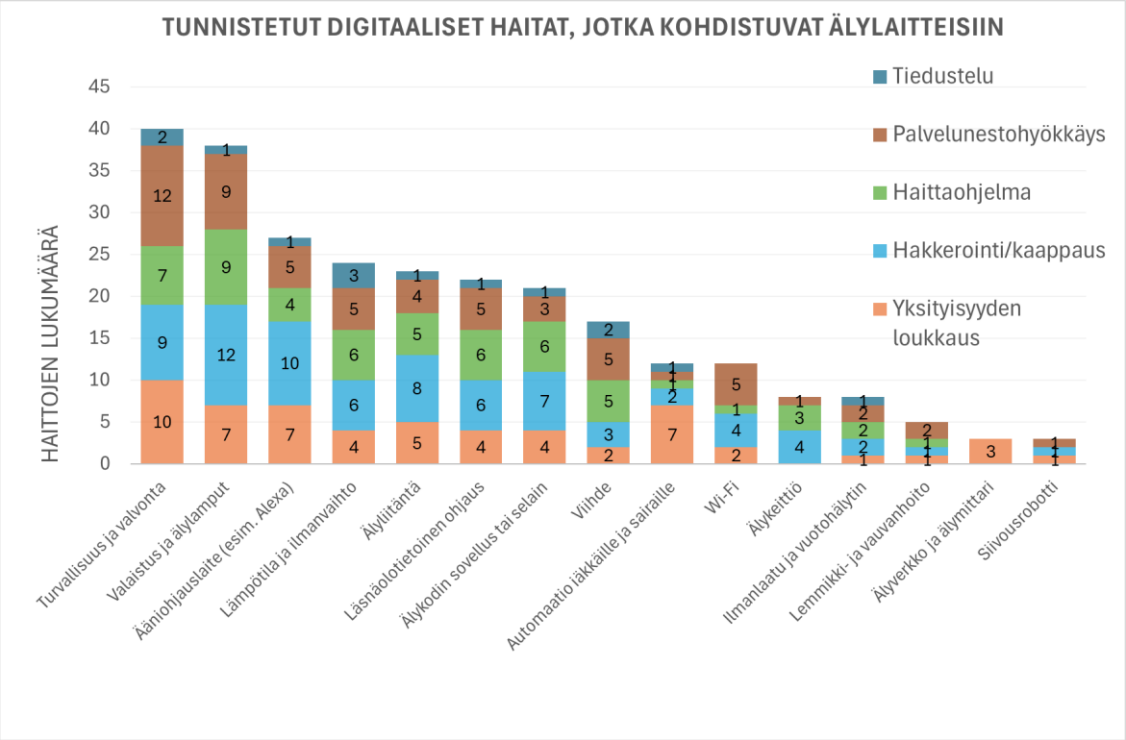
seuraaminen lisäävät tietoisuutta suojata älykoti (Touqeer ja muut, 2021 s. 14070). Myös muut suojautumismenetelmät kuten tietoliikenteen suodatus ja ohjelmistojen päivittäminen ovat tärkeitä sovelluskerroksen turvatoimia. Nämä menetelmät voi tehdä omiin IoT-laitteisiin automaattisiksi, jolloin ne eivät unohdu tehdä. Taulukko 1 kokoaa vielä älykoteihin kohdistuvat uhat, vaikutukset ja suojausmenetelmät yhteen.

Taulukko 1. Älykoteihin kohdistuvat uhat, vaikutukset ja suojausmenetelmät.

Älykoteihin kohdistuvat uhat	***Vaikutukset***	***Esimerkki hyökkäyksestä***	***Suojausmenetelmät***
Palvelunestohyökkäys (DoS, DDoS, PDoS)	Laitteiden ja palveluiden ylikuormitus, estäen normaalin toiminnan	Mirai-botnet hyökkäys	Palomuuri, tietoliikenteen suodatus
Salakuuntelu- ja tiedusteluhyökkäys	Tietovuodot, yksityisyyden loukkaus	Yksityinen hyökkäys, WiFi-verkon tiedustelu	VPN, WPA3-salaus, verkon segmentointi, laitteiden päivitys, mikrofonien ja kameroiden suojaus
Välimieshyökkäys	Tietoliikenteen manipulointi, tietojen vuoto	Evil Twin (MITM), sähköpostikaappaus	MAC-osoitteiden suodatus, HTTPS-protokollan käyttäminen, VPN, verkon suojaus, monivaihetunnistaminen
Huijaus- ja väärennöshyökkäys	Ulkopuolisen pääsy tunnuksiin, taloudelliset tappiot, identiteettivarkaudet, haittaohjelmat	Phishing, Spoofing	Yleinen tarkkaavaisuus, monivaihetunnistautuminen, käyttäjien tietoturvaosaaminen, suojausmekanismit (SPF, DKIM)
Haittaohjelmat	Laitteiden kaappaukset, häirintä, tietovarkaudet	Troijalainen, madot, ransomware	Palomuuri, ohjelmistojen päivittäminen, virustorjunta, varmuuskopiot
Häirintähyökkäykset	Laitteiden viestintähäiriöt, toimintahäiriöt	Jatkuva ja reaktiivinen taajuushäirintä	Suojatut viestintäkanavat, laitteiden pääsynhallinta, varayhteydet
Fyysiset hyökkäykset	Laitteiden rikkoutuminen, taloudelliset vahingot, varastaminen	Laitteiden varastaminen, tuhoaminen, ilkivalta, käyttövoiman katkaiseminen	Suojattu rakennesuunnittelu, fyysiset esteet, kamerat, vakuutus
Salasanamurrot	Salasanojen paljastuminen, tietomurrot	Brute Force	Vahvat ja yksilölliset salasanat, oletussalasanojen välttäminen, monivaihetunnistautuminen

4.3 Tilastokatsaus IoT-laitteiden riskeihin

Älykodeista on saatavilla rajoitetusti tilastollista tutkimustietoa, joka keskittyisi IoT-laitteiden haavoittuvuuksiin. Buil-Gilin ja muiden (2023) systemaattisessa kirjallisuuskatsauksessa tunnistettiin ja luokiteltiin älykoteihin kohdistuvia digitaalisia haittoja. Kuviossa 1 esitetään mukaelma älylaitteisiin kohdistuvista digitaalisista haitoista.



Kuvio 1. Tunnistetut digitaaliset haitat, jotka kohdistuvat älylaitteisiin (mukaelma lähteestä Buil-Gil ja muut, 2023).

Tutkimuksen analyysin mukaan yleisimmät älykoteihin kohdistuvat uhat olivat yksityisyyden loukkaukset (72,1 %), hakkerointi/kaappaus (67,4 %), haittaohjelmat (51,2 %) ja palvelunestohyökkäykset eli DoS/DDoS-hyökkäykset (48,8 %). Lisäksi tiedustelua esiintyi 7,0 %:ssa tapauksista (Buil-Gil ja muut, 2023, s. 14). Analyysin mukaan voidaan päätellä, että turvallisuus- ja valvontalaitteet ovat erityisen haavoittuvassa asemassa niihin kohdistuvien uhkien määrän takia. Ison haittaosuuden muodostaa esimerkiksi hakkerointi tai kaappaus (engl. hacking), joka meidän tutkimuksessamme viittaa esimerkiksi laitteiden välimieshyökkäykseen. Kuviosta

nähdään myös, että uhka kohdistuu todennäköisemmin suurempaan järjestelmään tai laitekokonaisuuteen, kuin yksittäisiin laitteisiin älykodissa. Hyvänä esimerkkinä voidaan pitää siivousrobotin osuutta verrattuna turvallisuusjärjestelmään älykodissa. Hyökkäämällä turvallisuusjärjestelmään, hyökkäyksen haittavaikutukset ovat paljon laajemmat.

Tutkimuksen perusteella voidaan vahvasti suositella, että käyttäjät ja laitevalmistajat panostavat erityisesti yksityisyyden suojaan, salasanojen ja tunnistautumisjärjestelmien vahvistamiseen sekä haittaohjelmien torjuntaan. Tämän numeerisen analyysin avulla tutkielmassa esitetyt johtopäätökset ja suositukset saavat selkeän empiirisen tuen, joka auttaa ymmärtämään älykotien kyberturvallisuuden käytännön haasteita ja ratkaisutarpeita.

4.4 Tulevaisuuden kehityssuunnat ja haasteet älykotien turvallisuudessa

Älykotien yleistyminen ja IoT-teknologian kehitys tuovat mukanaan uusia turvallisuushaasteita, mutta myös uusia mahdollisuuksia. Tulevaisuudessa laitteiden määrä ja niihin kohdistuvien hyökkäysten monimuotoisuus lisääntyvät entisestään. Tämä edellyttää jatkuvaa kehitystä ja mukautumista sekä käyttäjiltä että laitteiden valmistajilta. Kehittyvät tekoälypalvelut ja koneoppiminen ovat keskeisessä osassa tulevaisuuden kehityksessä hyvässä sekä pahassa. Tekoälypohjaiset (engl. Artificial Intelligence, AI) järjestelmät tuovat uusia turvallisuusratkaisuja niiden kehittyneiden tunnistus- ja analyysimenetelmien avulla. Esimerkiksi koneoppimista hyödyntävät järjestelmät kykenevät tunnistamaan poikkeavuuksia tietoliikenteessä ja reagoimaan niihin reaaliaikaisesti, parantaen näin älykodin kykyä estää hyökkäyksiä (Radanliev ja muut, 2024).

Tulevaisuuden yksi selkeä kehityssuunta on ollut tunnistautumisjärjestelmät. Useat palvelut ovat ottaneet käyttöönsä biometrisiä tunnistusjärjestelmiä. Tämä tarkoittaa sitä, että esimerkiksi älypuhelimen pääsykoodit ja muut tunnusluvut ovat vaihtuneet

sormenjälki- ja kasvojentunnistukseen. Tämä tuo laitteisiin lisää käyttömukavuutta, mutta myös turvallisuutta. Tämä uudistus on myös siirtymässä älykotiympäristöön, jossa avaimella toimivat ovet vaihdetaan koodisarjoihin tai sormentunnistuksiin.

Instituutillisia muutoksia on myös havaittavissa ohjeistuksissa ja säädöksissä. Euroopan unionin ja muut instituutiot pyrkivät parantamaan yleistä turvallisuuspolitiikkaa. Tämä voi näkyä tiukempina turvavaatimuksina ja erilaisten standardien kehityksenä. Esimerkiksi ISO 27001:2022 on kansainvälinen tietoturvallisuuden hallintajärjestelmän standardi, joka auttaa yrityksiä ja organisaatioita suojaamaan tietojaan systemaattisesti. Onkin yleistä, että älykoteja tuottavat yritykset pyrkivät lisäämään asukkaiden tietoturvallisuutta organisaatiotasolta asti. Tämä johtaa laitteiden pidempiin elinkaariin, säännöllisempiin ohjelmistopäivityksiin ja parempaan yleiseen turvallisuuteen.

Lisäksi Zero-Trust-mallin mukaiset suojaratkaisut voivat parantaa turvallisuutta älykodeissa hallinnoimalla entistäkin tarkemmin käyttöoikeuksia järjestelmiin (Ameer ja muut, 2022). Tämä tarkoittaa käytännössä jatkuvaa todennusta, mikä vähentää huomattavasti hyökkäyksen mahdollisuutta, vaikka yksittäinen laite tai tunnus vaarantuisi. Laite tai järjestelmä ei siis luota kehenkään ilman tunnistautumista. Pääsyoikeuksia arvioidaan jatkuvasti ja niitä voidaan peruuttaa reaaliaikaisesti, jos järjestelmä havaitsee epäilyttävää toimintaa. Tämä parantaa myös valvontaa ja kontrollointia älykodissa. Älykotijärjestelmät voivat lähettää hälytyksiä, jos epäilyttävää toimintaa havaitaan ja tuntematon laite yrittää liittyä verkkoon.

Älykotien turvallisuuden haasteet nousevat myös esille tulevaisuudessa. IoT-laitteiden kasvavan määrän myötä älykotien hyökkäyspinta-alakin kasvaa. Hyökkääjien mahdollisuus löytää haavoittuvuuksia ja hyödyntää niitä tulevaisuudessa tulee olemaan yleisempää. Tämä voi tuoda myös toisen haasteen esille, joka ilmenee ihmisten tietoturvaosaamisen puutteellisuudessa. IoT-laitteiden nopea tekninen kehitys haastaa käyttäjien tietoturvaosaamista. Varsinkin iäkkäämmät käyttäjät saattavat kohdata haasteita hahmottaa uusien laitteiden ja sovellusten toimintaa, mikä lisää riskiä joutua

tietojenkalastelun ja huijauksen kohteeksi. Lisäksi ihmisten sosiaalisen media käyttö ja jatkava oman elämän taltiointi ja jakaminen internetissä antaa hyökkääjille hyvät perustiedot kohteeseensa.

Kyberrikollisuuden kehitys on merkittävä haaste älykotien tulevaisuudessa. Kyberrikolliset panostavat jatkuvasti enemmän teknologiaan ja taloudellisesti yhä enemmän hyökkäyksien laatuun ja määrään (Griffiths, 2025). Varsinkin tekoälyn hyödyntäminen rikollisissa tarkoituksissa on yleistynyt. Tekoälyn avulla kehitellään esimerkiksi palvelunestohyökkäyksiä ja kalastelumassaviestejä. Botnettien kasvavat koot ja hyökkäysteho ovat merkittäviä uhkia tulevaisuudessa. Esimerkiksi Mirai-botnetin kaltaiset verkostot voivat jo nyt yhdistää satojatuhansia laitteita samaan hyökkäykseen (Angrishi, 2017, s. 6). Vaikka tietokoneiden järjestelmien salaustekniikat kehittyvät, samalla myös niiden murtautumiskeinot parantuvat.

5 Johtopäätökset

Tässä kandidaatintutkielmassa tavoitteena oli tunnistaa ja analysoida, millaisia uhkia IoT-laitteisiin kohdistuu ja millä tavoin näitä uhkia voidaan torjua älykotiympäristössä. Tavoitteena oli myös tarjota suosituksia, joiden avulla älykotien kyberturvallisuutta voidaan parantaa ja kuinka suojata omia IoT-laitteita konkreettisilla toimilla. Älykotien yleistyminen ja teknologian jatkuva kehitys johtavat muutoksiin arjen toiminnallisuudessa, mutta samalla ne ovat tuoneet kasvavia tietoturvahaasteita. Tutkimuksen havaintojen mukaan älykotien turvallisuusuhat ovat todellisia ja ne ovat kasvava ilmiö. Kirjallisuustutkielmassa havaittiin yleisimpinä kyberturvahaavoittuvuuksina käyttäjien puutteellinen tietotaitotaso, laitteiden riittämätön suojaus ja teknologinen heterogeenisyys älykotiympäristössä. Lisäksi IoT-laitteiden turvallisuustasossa on merkittäviä eroja valmistajien ja mallien välillä, mikä vaikeuttaa yhtenäisten turvallisuusstandardien luomista. Vaikka älykotien IoT-laitteet ovat haavoittuvaisia kyberuhille, niiden suojautumismenetelmiä kehitellään jatkuvasti paremmiksi.

Tutkimuksen perusteella älykoteihin kohdistuvat hyökkäysvektorit ovat monimuotoisia, ja niiden seuraukset voivat olla hyvinkin merkittäviä. Yleisimpinä hyökkäystyyppeinä tunnistettiin palvelunestohyökkäykset, tiedustelu- ja salakuunteluhyökkäykset, välimieshyökkäykset, huijaus- ja kalasteluhyökkäykset, haittaohjelmat, häirintähyökkäykset sekä fyysiset hyökkäykset. Näistä erityisesti hajautetut palvelunestohyökkäykset ja haittaohjelmapohjaiset hyökkäykset, kuten botnet-hyökkäykset ovat osoittautuneet erittäin haitallisiksi, sillä ne voivat lamauttaa kokonaisia järjestelmiä ja aiheuttaa pitkäkestoisia häiriöitä älykotiympäristöissä.

Tutkimuksessa käsiteltiin myös yleisiä suojautumismenetelmiä, joiden avulla voidaan vähentää hyökkäyksiä. Keskeisiä suojautumismenetelmiä, joita voidaan soveltaa älykodin kyberturvan parantamiseksi, ovat vahvojen salasanojen käyttö, monivaihetunnistautuminen, tietoliikenteen salausmenetelmät, ohjelmistojen säännöllinen päivittäminen sekä palomuurien ja virustorjuntaohjelmistojen

hyödyntäminen. Fyysisiä suojautumistoimia, kuten valvontajärjestelmiä ja laitteiden fyysistä suojausta ilkivaltaa vastaan, ovat myös yksi keskeinen osa älykotien turvallisuudessa. Yhteenvetona voidaan todeta, että älykotien IoT-laitteiden tietoturva edellyttää sekä teknologisia ratkaisuja että käyttäjäkohtaisia toimenpiteitä. Laitteiden valmistajilla on merkittävä vastuu turvallisuusratkaisujen sisällyttämisestä laitteisiin jo suunnitteluvaiheessa, mikä voisi vähentää kyberhyökkäyksien onnistumisia ja niiden mahdollisuuksia. Vastaavasti käyttäjien oma aktiivisuus ja tietoturvatietoisuuden lisääminen on välttämätöntä kokonaisvaltaisen turvallisuuden varmistamiseksi.

5.1 Suositukset oman älykodin turvallisuuden parantamiseen

Älykodissa on hyvin paljon erilaisia haavoittuvuuksia IoT-laitteiden rajapinnalla. Kodin laitteet väärinkäytettynä voivat olla selkeä turvallisuusuhka. Kokosimme tutkimukseen taulukkoon 2 omat suosituksemme älykodin turvallisuuden parantamiseksi. Suositukset perustuvat tutkielmassa käsiteltyihin tutkimuksiin sekä niiden pohjalta muodostettuihin johtopäätöksiin. Näiden konkreettisien toimien myötä, älykotien kyberturvallisuus parantuu huomattavasti ja hyökkäysuhkien mahdollisuus vähenee merkittävästi.

Taulukko 2. Älykodin omistajan tarkistuslista kodin turvallisuuden varmistamiseksi.

	Älykodin omistajan tarkistuslista kodin turvallisuuden varmistamiseksi
1	Käytä vahvoja ja yksilöllisiä salasanoja laitteisiin ja palveluihin, älä käytä oletussalasanoja.
2	Muista hyödyntää monivaihetunnistautumista (MFA) kaikissa mahdollisissa palveluissa.
3	Päivitä laitteiden ohjelmistot säännöllisesti.
4	Poista tarvittaessa IoT-laitteiden etähallinta ja vältä suojaamattomia etäyhteyksiä.
5	Käytä palomuureja, salaustekniikoita (WPA3), virustorjuntaohjelmia ja VPN-sovelluksia.
6	Älä jaa pääsykoodeja tai muita arkaluontoisia tunnuksia epäilyttäville sivustoille.
7	Varmista fyysinen turvallisuus asentamalla valvontakameroita ja hälytysjärjestelmiä.
8	Lisää omaa tietoisuutta kyberturvallisuudesta seuraamalla tietoturvauutisia.
9	Ota ammattilaiseen yhteyttä hyökkäyksen sattuessa.

5.2 Tutkimuksen rajoitukset ja jatkotutkimuksen mahdollisuudet

Tämä tutkielma toteutettiin kirjallisuuskatsauksena, mikä rajoittaa sen tuloksia kirjallisuuden saatavuuteen ja ajankohtaisuuteen. Tutkielmassa nousi useasti alueen laajuus yhdeksi rajoitteeksi. Aihealue on hyvin laaja, ja aiheen eri osa-alueita olisi mahdollista tutkia huomattavasti syvemmin. Esimerkiksi pelkästään älykotien hyökkäysvektorit tai suojautumismenetelmät voisivat olla täysin omia tutkimusaiheitaan. Toinen merkittävä rajoite tutkielmassa liittyi informaation ja datan saatavuuteen, koska aiheena älykodit ovat yhteiskunnallisesti uusia ja monesti niihin liittyvät artikkelit ovat suppeita. Vaikka älykotien turvallisuutta tutkitaankin jatkuvasti, on luotettava tilastollinen tutkimus edelleen kapeaa. Kaupalliset yritykset selvittävät haavoittuvuuksia ja hyökkäystapoja älykoteihin, mutta nämä eivät kuitenkaan tue tutkimuksiaan aina akateemisesti. Tilastot ja prosentuaaliset osuudet näytetään usein ilman lähdeviittauksia ilman lisäselvityksen mahdollisuutta. Tutkimukset vaihtelevat vuosittain ja tutkimuskohteet voivat muuttua otannan mukaan.

Tutkielman jatkotutkimusmahdollisuudet ovat siis hyvin laajat. Tulevissa tutkimuksissa voisi syventyä pohtimaan älykotien parannustoimia ja nykyisiä haavoittuvuuksia laite- tai järjestelmäkohtaisesti. Hyökkäysvektoreiden tarkempi analysointi älykodeissa tarjoaisi myös kiinnostavia näkökulmia. Lisäksi tutkimustyö etenkin yritykselle, joka kehittää älykoteja ja niiden sovelluksia, olisi arvokasta. Tämä antaisi mahdollisuuden päästä tarkastelemaan turvallisuusuhkia ja niiden torjuntaa käytännössä, jossa voitaisiin tehdä kokeellisia testejä ja tarkempia tapaustutkimuksia älykotien IoT-laitteiden tietoturvasta. Kyseessä on erittäin ajankohtainen tutkimusalue, jonka merkitys tulee kasvamaan teknologian kehittymisen ja IoT-laitteiden yleistymisen myötä. Tästä syystä aiheeseen liittyvä jatkotutkimus on erittäin perusteltua ja tärkeää yhteiskunnan kokonaisvaltaisen turvallisuuden näkökulmasta.

Lähteet

Abaimov, S. (2024, toukokuu 11). Understanding and Classifying Permanent Denial-of-Service Attacks. *Journal of CyberSecurity and Privacy*, 4(2), (s. 324–339). https://doi.org/10.3390/jcp4020016

Abdullah, T. A.A., Ali, W., Malebary, S. & Ahmed, A. A. (2019, syyskuu). A Review of Cyber Security Challenges, Attacks and Solutions for Internet of Things Based Smart Home. *IJCSNS,* 19(9), Noudettu 25. helmikuuta 2025 osoitteesta https://www.researchgate.net/publication/336717887_A_Review_of_Cyber_Security_Challenges_Attacks_and_Solutions_for_Internet_of_Things_Based_Smart_Home

Aldahmani, A., Ouni, B., Lestable, T. & Debbah, M. (2023, tammikuu 4). Cyber-Security of Embedded IoTs in Smart Homes: Challenges, Requirements, Countermeasures, and Trends. *IEEE Open Journal of Vehicular Technology,* 4, (s. 281–292). 10.1109/OJVT.2023.3234069

Ali, B. & Awad, A.I. (2018, maaliskuu 6). Cyber and physical security vulnerability assessment for IoT-based smart homes. *Sensors, 18*(3), 817. Noudettu 23. helmikuuta 2025 osoitteesta https://www.mdpi.com/1424-8220/18/3/817

Alrawi, O., Lever, C., Antonakakis, M. & Monrose, F. (2019, toukokuu 20). SoK: Security evaluation of home-based IoT deployments. *In 2019 IEEE Symposium on Security and Privacy*. IEEE. Noudettu 23. helmikuuta 2025 osoitteesta https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8835392

Alshamsi, O., Shaalan, K. & Butt, U. (2024, lokakuu 13). Towards securing smart homes: A systematic literature review of malware detection techniques and recommended prevention approach. *Information,* 15(10), 631. https://doi.org/10.3390/info15100631

Ameer, S., Gupta, M., Bhatt, S. & Sandhu, R. (2022, kesäkuu 8). BlueSky: Towards convergence of zero trust principles and score-based authorization for IoT enabled smart systems. *SACMAT '22: Proceedings of the 27th ACM on Symposium on Access Control Models and Technologies.* (s. 235–244). https://doi.org/10.1145/3532105.3535020

Anand, P., Singh, Y., Selwal, A., Alazab, M., Tanwar, S. & Kumar, N. (2020). IoT Vulnerability Assessment for Sustainable Computing: Threats, Current Solutions, and Open Challenges. *IEEE Access,* 8, (s. 168825–16885). 10.1109/ACCESS.2020.3022842

Angrishi, K. (2017). Turning Internet of Things (IoT) into Internet of Vulnerabilities (IoV): IoT botnets. *arXiv preprint* arXiv:1702.03681. https://doi.org/10.48550/arXiv.1702.03681

Arabo, A. (2015). Cyber Security Challenges within the Connected Home Ecosystem Futures. *Procedia Computer Science,* 61, (s. 227–232) https://doi.org/10.1016/j.procs.2015.09.201

Barnes, D. (2020, maaliskuu 20). Redefining That Makes A Smart Home 'Smart'. Noudettu 25. helmikuuta 2025 osoitteesta: https://www.forbes.com/sites/forbesrealestatecouncil/2020/03/20/redefining-what-makes-a-smart-home-smart/?sh=11fffc491832.

Brass, I., Tanczer, L., Carr, M., Elsden, M. & Blackstock, J. (2018, kesäkuu). Standardising a moving target: The development and evolution of IoT security standards. *Living in the Internet of Things: Cybersecurity of the IoT - 2018*. https://doi.org/10.1049/cp.2018.0024

Buil-Gil, D., Kemp, S., Kuenzel, S., Coventry, L., Zakhary, S., Tilley, D. & Nicholson, J. (2022, elokuu 22). The digital harms of smart home devices: A systematic literature review. *Computers in Human Behavior,* 145. https://doi.org/10.1016/j.chb.2023.107770

Christie, J. (2014, huhtikuu 27). 'Wake up baby!' The chilling words U.S. couple heard in the middle of the night from a man who had hacked their daughter's baby monitor and was WATCHING her sleep, *DailyMail Online News.* 2614462, Noudettu 13. huhtikuuta 2025 osoitteesta https://www.dailymail.co.uk/news/article-2614462/Wake-baby-The-chilling-words-couple-heard-middle-night-man-hacked-daughters-baby-monitor-WATCHING-sleep.html

Cyber-Recon. (2020, huhtikuu 28). *Security + 1.2 Wireless Jamming* [video]. YouTube. Noudettu 10.3.2025 osoitteesta https://www.youtube.com/watch?v=9ctepkAu8KU&t=19s

Estrada, D., Tawalbeh, L. & Vinaja, R. (2020, maaliskuu 19). How Secure Having IoT Devices in Our Homes? *Journal of Information Security,* 11, (s. 81–91). https://doi.org/10.4236/jis.2020.112005

Gazis, A. (2021, kesäkuu 7). What is IoT? The Internet of Things explained. *Academia Letters,* 1003, (s. 1–8). https://doi.org/10.20935/AL1003

Griffiths, C. (2025, tammikuu 1). The Latest 2025 Phishing Statistics (updated January 2025), *AGG IT.* Noudettu 18. maaliskuuta 2025 osoitteesta https://aag-it.com/the-latest-phishing-statistics/

Gupta, B. B., Tewari, A., Jain, K. A. & Agrawal, D. P. (2016, maaliskuu 17). Fighting against phishing attacks: state of the art and future challenges. *Neural Computing and Applications,* 28, (s. 3629–3654). Noudettu 18. maaliskuuta 2025 osoitteesta: https://link.springer.com/article/10.1007/s00521-016-2275-y#citeas

Hammi, B., Zeadally, S., Khatoun, R. & Jamel, N. (2022). Survey on smart homes: Vulnerabilities, risks, and countermeasures. *Computers & Security,* 117(2), 102677. https://doi.org/10.1016/j.cose.2022.102677

Ho, G., Leung, D., Mishra, P., Hosseini, A., Song, D. & Wagner, D. (2016 toukokuu, 30). Smart Locks: Lessons for Securing Commodity Internet of Things Devices, *University of California, Berkeley*, https://doi.org/10.1145/2897845.2897886

Huraj, L., Šimon, M. & Horák, T. (2020, syyskuu 16). Resistance of IoT sensors against DDoS attack in smart home environment. *Sensors,* 20(18), 5298. https://doi.org/10.3390/s20185298

Kavallieratos, G., Chowdhury, N., Katsikas, S., Gkioulus, V. & Wolthusen, S. (2019 syyskuu 25). Threat Analysis for Smart Homes, *MDPI Open Access Journal, future internet,* 11(10), 207. https://doi.org/10.3390/fi11100207

Khan, W. Z., Zahid, M., Aalsalem, M. Y., Zangoti, H. M. & Arshad, Q. (2018, kesäkuu 29). Ethical aspects of Internet of Things from Islamic perspective. *Cornell University, Computers and Society.* 10.48550/arXiv.1806.11386

Kofler, M. J., Reinisch, C. & Kastner, W. (2012 huhtikuu). A semantic representation of energy-related information in future smart homes. *Energy and Buildings*, 47, (s. 169-179). https://doi.org/10.1016/j.enbuild.2011.11.044

Kumar, K., Sen, N., Azid, S. & Mehta, U. (2016, joulukuu). A Fuzzy Decision in Smart Fire and Home Security System. *IEEE International Symposium on Robotics and Intelligent Sensors.* https://doi.org/10.1016/j.procs.2017.01.207

Lindsay, G., Woods, B. & Corman, J. (2016, maaliskuu 30). Smart homes and the internet of things. *Atlantic Council.* Noudettu 27. helmikuuta 2025 osoitteesta: https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/smart-homes-and-the-internet-of-things/

Linnake, T. & Kärkkäinen, H. (2025, maaliskuu 18). Onko kotonasi tällainen reititin? Tarkista päivitykset – hyökkäykset käynnissä, *IltaSanomat, DigiToday, Tietoturva.* Noudettu 19. maaliskuuta 2025 osoitteesta: https://www.is.fi/digitoday/tietoturva/art-2000011103710.html

Mahlous, A. R. (2022, marraskuu 21). Threat model and risk management for a smart home IoT system. *Informatica,* 47(1), (s. 51–64). https://doi.org/10.31449/inf.v47i1.4526

Mallik, A. (2018, lokakuu). Man-in-the-middle-attack: Understanding in simple words. *Cyberspace: Jurnal Pendidikan Teknologi Informasi,* 2(2), (s. 109–134). Noudettu 16. maaliskuuta 2025 osoitteesta: https://jurnal.ar-raniry.ac.id/index.php/cyberspace/article/view/3453/2707

Neshenko, N., Bou-Harb, E., Crichigno, J., Kaddoum, G. & Ghani, N. (2019, huhtikuu 11). Demystifying IoT security: An exhaustive survey on IoT vulnerabilities and a empirical look on internet-scale IoT exploitations. *IEEE Communications Surveys & Tutorials,* 21(3), (s. 2702–2733). https://doi.org/10.1109/COMST.2019.2910750

Nirmal, K., Janet, B. & Kumar, R. (2020, kesäkuu 20) Analyzing and eliminating phishing threats in IoT, network and other Web applications using iterative intersection, *Peer-to-Peer Networking and Applications,* 14. (s. 2327–2339). Noudettu 18

maaliskuuta 2025 osoitteesta https://link.springer.com/article/10.1007/s12083-020-00944-z

Ouramdane, O., Elbouchikhi, E., Amirat, Y., Le Gall, F. & Gooya, E. S. (2022, huhtikuu 13). Home energy management considering renewable resources, energy storage, and an electric vehicle as a backup. *Energies,* 15(8), 2830. https://doi.org/10.3390/en15082830

Panay, P. (2025, helmikuu 26). Introducing Alexa+, the next generation of Alexa, *Amazon News SVP of Devices & Services.* Noudettu 27. helmikuuta 2025 osoitteesta: https://www.aboutamazon.com/news/devices/new-alexa-generative-artificial-intelligence

Plachkinova M. & Vo A., Alluhaidan A. (2016, heinäkuu 11). Emerging Trends in Smart Home Security, Privacy, and Digital Forensics, *Twenty-second Americas Conference on Information Systems.* Noudettu 20. helmikuuta 2025 osoitteesta: https://web.archive.org/web/20200323123821id_/https://aisel.aisnet.org/cgi/viewcontent.cgi?referer=&httpsredir=1&article=1434&context=amcis2016

Radanliev, P., De Roure, D., Maple, C., Nurse, J. R. C., Nicolescu, R. & Ani, U. (2024, lokakuu 10). AI security and cyber risk in IoT systems. *Frontiers in Big Data*, 7. https://doi.org/10.3389/fdata.2024.1402745

Rikoslaki 21.4.1995/578. Finlex. Noudettu 11.3.2025 osoitteesta: https://finlex.fi/fi/lainsaadanto/1889/39-001

Rao, T.A. & Haq, E. (2018, maaliskuu). Security challenges facing IoT layers and its protective measures, *International Journal of Computer Applications,* 179*,* (s. 31–35). http://dx.doi.org/10.5120/ijca2018916607

Roman, R., Zhou, J. & Lopez, J. (2013, heinäkuu). On the features and challenges of security and privacy in distributed internet of things, *Computer Networks,* 57, (s. 2266–2279). https://doi.org/10.1016/j.comnet.2012.12.018

Rouillard, J. (2013, toukokuu 22). The Pervasive Fridge. A smart computer system against uneaten food loss, *Seventh International Conference on Systems (ICONS2012)*, (s. 135–140). Noudettu 1. maaliskuuta 2025 osoitteesta https://hal.science/hal-00825886/

Sangeetha, T., Kumutha, D., Bharathi, M.D. & Surendran, R. (2022, joulukuu). Smart mattress integrated with pressure sensor and IoT functions for sleep apnea detection, *Measurement: Sensors,* 24. https://doi.org/10.1016/j.measen.2022.100450

Sikder, A. K., Petracca, G., Aksu, H., Jaeger, T. & Uluagac, A. S. (2018, helmikuu 5). A survey on sensor-based threats to internet-of-things (IoT) devices and applications. http://dx.doi.org/10.48550/arXiv.1802.02041

Sovacool, B. K. & Furszyfer Del Rio, D. D. (2020, maaliskuu). Smart home technologies in Europe: A critical review of concepts, benefits, risks and policies, *Renewable and Sustainable Energy Reviews,* 120*.* https://doi.org/10.1016/j.rser.2019.109663

Statista Research Department. (2025, helmikuu 24). Number of users of smart homes worldwide 2019–2028. *Statista.* Noudettu 25 helmikuuta 2025, osoitteesta https://www.statista.com/forecasts/887613/number-of-smart-homes-in-the-smart-home-market-in-the-world

Touqeer, H., Zaman, S., Amin, R., Hussain, M., Al-Turjman, F. & Bilal, M. (2021, toukokuu 10). Smart home security: challenges, issues and solutions at different IoT layers, *The Journal of Supercomputing.* https://doi.org/10.1007/s11227-021-03825-1

Vailshery, L. S. (2024, helmikuu 11). Number of IoT connections worldwide 2022–2033. *Statista Research Departmant.* Noudettu 25. helmikuuta 2025, osoitteesta https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/

Xia, H. & Brustoloni, J.C. (2005, toukokuu 10). Hardening Web browsers against man-in-the-middle and eavesdropping attacks, *WWW '05: Proceedings of the 14th international conference on World Wide Web,* (s. 489–498). https://doi.org/10.1145/1060745.1060817

Yasar, K. & Shea, S. (2023, elokuu). Definition smart home, *Tech Target Network*, Noudettu 18. maaliskuuta 2025 osoitteesta https://www.techtarget.com/iotagenda/definition/smart-home-or-building

Zhou, B., Li, W., Chan, K., W., Cao, Y., Kuang, Y., Liu, X. & Wang, X. (2016, elokuu). Smart home energy management systems: Concept, configurations, and scheduling strategies. *Renewable and Sustainable Energy Reviews,* 61, (s. 30–40). https://doi.org/10.1016/j.rser.2016.03.047