Eetu Kattelus

Koneoppimisen hyödyntäminen esineiden internetin kyberturvallisuudessa

Tietotekniikan kandidaatintutkielma

16. toukokuuta 2023

Jyväskylän yliopisto

Informaatioteknologian tiedekunta

Tekijä: Eetu Kattelus

Yhteystiedot: eemikatt@student.jyu.fi

Ohjaaja: Rossi, Tuomo

Työn nimi: Koneoppimisen hyödyntäminen esineiden internetin kyberturvallisuudessa

Title in English: Utilization of machine learning in the cyber security of the Internet of Things

Työ: Kandidaatintutkielma

Opintosuunta: Tietotekniikka

Sivumäärä: 24+0

Tiivistelmä: Esineiden internet koostuu toisiinsa verkon välityksellä kommunikoivista laitteista. Kyberturvallisuus näissä laitteissa on usein riittämätön, mikä olisi tärkeää saada ajan tasalle laitteiden alati kasvavan määrän vuoksi. Koneoppimista pidetään yhtenä mahdollisena vastauksena tässä sekä yleisesti kyberturvallisuuden ylläpitämisessä ja parantamisessa. Tässä tutkielmassa on tarkoitus tutkia, miten koneoppimista voitaisiin hyödyntää esineiden internetin kyberturvallisuuden parantamisessa.

Avainsanat: Kyberturvallisuus, esineiden internet, Koneoppiminen, Tekoäly

Abstract: The Internet of Things consists of devices that communicate with each other via a network of some sort. Cyber security in these devices is often insufficient, which should be kept up to date with the ever-increasing number of such devices. Machine learning is seen as one possible answer to this, and to maintaining and improving cyber security in general. The purpose of this bachelor's thesis is to investigate how machine learning could be used in improving the cyber security of the Internet of Things.

Keywords: cyber security, Internet of things, IoT, Machine Learning, ML, Artificial intelligence, AI

Eetu Mikael Kattelus

Kuviot

Taulukot

Sisällys

1 Johdanto

Esineiden internetillä (engl. *Internet of Things*, *IoT*) tarkoitetaan fyysisiä esineitä, jotka ovat yhteydessä toisiinsa sekä mm. jakavat dataa keskenään jonkinlaisen verkon, kuten internetin, välityksellä. Ciscon tekemän tutkimuksen ("Cisco Annual Internet Report" 2020) mukaan IP-verkkoihin olisi vuoteen 2023 mennessä kytkettynä yli 29 miljardia laitetta, kun määrä oli vielä vuonna 2018 yli 18 miljardia. Puolet näistä yhteyksistä olisivat laitteiden välisiä (engl. *Machine-to-Machine*).

Esineiden internetin suuri määrä ei kuitenkaan tule välttämättä suurena yllätyksenä, sillä nykyään yhä useampi laite on yhteydessä internetiin ja älypuhelimeesi. Esineiden internetistä on muitakin hyötyjä, kuin arkipäiväisen elämän helpottamista, sillä näiden laitteiden avulla voidaan kerätä hyvinkin tärkeää dataa. Esineiden internetin avulla myös kokonaiset kaupungit ja niiden infrastruktuurit voivat toimia tehokkaammin, joko yksinään tai yhteydessä toisten kaupunkien kanssa.

Tutkielman aihe on ajankohtainen, sillä esineiden internetin nopea kasvu johtaa myös välttämättä kyberhyökkäysten ja -murtojen nousuun. *IoT*-laitteiden kyberturvallisuuden varmistaminen onkin haastavaa niiden pienen laskentatehon sekä muistin vuoksi (Ali ym. 2021). Yhden laitteen suojaaminen voi vaikuttaa jopa turhalta, mutta esimerkiksi bottiverkkoja hyväksi käyttäen pientäkin laskentatehoa voidaan käyttää hyväksi suurissa määrissä. Esineiden internetissä saattaa liikkua hyvinkin arkaluotoista tietoa: kodin verkon tiedoista aina ihmisten sairaanhoitotietoihin.

Myös tekoäly – ja tätä kautta koneoppiminen, joka on tekoälyn osa-alue (Alzubaidi ym. 2021) – on ollut jo jonkin aikaa ajankohtainen ja tärkeä aihe. Tekoäly on myös tullut entistä selvemmin valtavirran tietoon *deepfake*:ien (syväoppimista hyödyntävää kuvien ja videoiden manipulointia) ja *chatGPT*:n (tekoälyä hyödyntävä chatbot) myötä, ellei jo aiemmin. Tekoälyn nopea kehittyminen saattaakin tuoda suuria muutoksia tapoihin ajatella tietokoneita, sekä luoda uusia mahdollisuuksia kyberturvallisuudelle, sekä uhkia sitä vastaan.

Tutkielma on tyypiltään kirjallisuuskatsaus. Lähteet on etsitty pääosin Scopuksen tietokantojen avulla, sekä artikkeleiden ja muiden tekstien julkaisukanavien luotettavuus on tarkastettu

pääosin julkaisufoorumin avulla. Lähteinä on myös pyritty käyttämään mahdollisimman tuoreita artikkeleita ym., mutta pääasiallisina lähteinä olen pyrkinyt käyttämään niin sanotusti ”varmempia” lähteitä.

Tutkimuskysymyksenä tutkielmassa on, millaisia kyberuhkia esineiden internetillä on, sekä kuinka koneoppimista voidaan hyödyntää esineiden internetin kyberturvallisuuden parantamiseen.

Tässä tutkielmassa tutkitaan esineiden internetin kyberturvallisuutta, sekä miten koneoppiminen ja tekoäly tulee vaikuttamaan siihen. Luvut 2, 3 ja 4 antavat teoreettisen pohjan tutkielmalle esineiden internetistä, kyberturvallisuudesta, sekä tekoälystä ja tarkemmin koneoppimisesta. Luvussa 5 tarkastellaan itse tutkimuksen aihetta, eli millainen kyberturvallisuus on esineiden internetissä tällä hetkellä, sekä kuinka koneoppiminen voi siihen vaikuttaa. Luku 6 on tutkielman yhteenveto.

2 Esineiden internet

Nimitystä ”internet of things” käytettiin luultavasti ensimmäisen kerran vuonna 1999 kuvaamaan RFID:n (*radio frequency identification*) avulla yhteyksissä oleviin laitteisiin (Ashton 2009). Nykyään esineiden internetiin yhteydessä olevia laitteita löytyy monessa eri muodossa. ”Älykodista” löytyvä tv, jääkaappi, valvontakamera ja jopa ulko-oven lukko voivatkin olla yhteydessä samaan esineiden internetin alustaan (Ali ym. 2021). Tässä luvussa tullaan määrittelemään esineiden internetin rakenne, sekä esittelemään joitain sen käyttötarkoituksia.

2.1 Esineiden internetin rakenne

Esineiden internetin rakenteesta ei ole päästy yhteisymmärrykseen, ja eri tutkijat ovat ehdottaneet erilaisia malleja (Sethi ja Sarangi 2017). Esineiden internet rakenne esitetään yleensä joko kolmi-, neljä- tai viisikerroksisella mallilla (ks. kuva 1), mutta jopa kahdeksankerroksisia arkkitehtuureja on ehdotettu (Zhou ym. 2021). Kolmikerroksisessa mallissa on havaintokerros (*perception layer*), verkkokerros (*network layer*) sekä sovelluskerros (*application layer*).

Havaintokerros on laitteiden fyysinen kerros. Ali ym. (2021) mukaan tämä kerros on kuin ihmisen tuntoelimet: silmät, jotka näkevät, korvat jotka kuulevat ja nenä joka haistaa. Tällä kerroksella siis laitteiden sensorit ym. osat ovat vuorovaikutuksessa ympäristön kanssa, sekä tuottavat kaikesta kerätystä datasta järkevää tietoa, jonka se antaa verkkokerrokselle liikuteltavaksi.

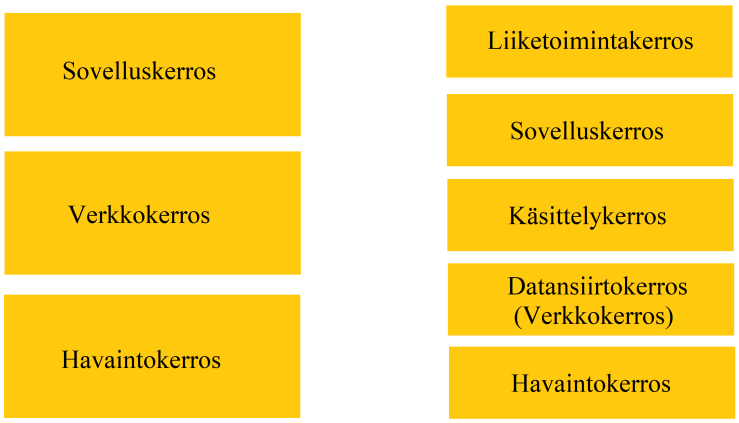
Verkkokerrosta kutsutaan joskus myös datansiirtokerrokseksi (engl. *data transmission layer*, myös *transportation layer*) (Ali ym. 2021). Tämän kerroksen työnä on ottaa data havaintokerrokselta, ja siirtää se ympäri esineiden internetiä langallisesti tai langattomasti, kuten varashälyttimen ilmoitukset suoraan päätelaitteeseen. Näin ollen verkkokerros siis toimii eräänlaisena siltana havaintokerroksen ja sovelluskerroksen välillä.

Sovelluskerroksen työnä on välittää tieto ja muita sovelluskohtaisia palveluita loppukäyttä-

jälle, ottamalla tarvittavan tiedon palvelimilta ja pilvipalveluilta (Ali ym. 2021). Useat arkiset älylaitteet kuten älykellot ja älytelevisiot käyttävät hyväkseen sovelluskerrosta. Kolmikerroksinen malli onkin hyvä, mutta hieman yksinkertainen tapa esittää esineiden internetin rakenne. Muun muassa Sethi ja Sarangi (2017) väittävätkin, että kolmikerroksinen malli ei ole tarpeeksi riittävä esineiden internetin tutkimukseen, koska tutkimuksessa keskitytään yleensä sen hienojakoisempiin puoliin. Näin ollen he ja monet muutkin tutkija ovat ehdottaneet useita eri hienojakoisempia malleja, joista seuraavaksi tullaan syventymään viisikerroksiseen malliin.

Viisikerroksisessa mallissa kerroksia tuleekin kaksi lisää: liiketoimintakerros (*business layer*) ja käsittelykerros (*processing layer*, myös *middleware layer*). Liiketoimintakerros toimii eräänlaisena esimiehenä esineiden internetille. Tällä kerroksella tapahtuu mm. sovellusten hallinta, liiketoiminnan kulku ja mallit sekä data luonti ja tallennus (Ali ym. 2021).

Käsittelykerroksessa tapahtuu datan käsittely, kun se ottaa sen vastaan datansiirtokerrokselta. Tällä kerroksella datasta siis valitaan vain halutut kohdat, sekä se muutetaan haluttuun ja käyttäjälle hyödylliseen muotoon sovelluskerrokselle vastaanotettavaksi. Käsittelyyn käytetään useita eri teknologioita, kuten eri tietokantoja ja pilvilaskentaa (Sethi ja Sarangi 2017).



Kuvio 1. Kolmi- ja viisikerroksinen malli (Sethi ja Sarangi 2017) mukaisesti esitettynä.

2.2 Esineiden internetin käyttötarkoitukset

Kuluttajille tarkoitetut IoT-laitteet ovat jatkuvasti kasvava osa esineiden internetiä. Jo aiemmin mainitut älykodit yleistyvät, kun laitteiden käytöt lisääntyvät. Williams, Terence J ja Immaculate (2019) jakoivat artikkelissaan älykodin laitteet kahteen kategoriaan: IoT-laitteesiin perustuva älykodin automaatio, sekä IoT-laitteisiin perustuvat älykodin turvajärjestelmät.

Älykodin automaatiolla tarkoitetaan käyttäjän mahdollisuutta hallita ja seurata eri älylaitteita halutessaan etäältä. Älykodin laitteita voidaan ohjata erilaisilla alustoilla, kuten siihen tarkoitetulla sovelluksella, tai erillisellä laitteella (*Amazon Echo*,*Google Home* ym.)

Älykodin turvajärjestelmillä taas tarkoitetaan taas erilaisia liiketunnistimia ja valvontakameroita. Käyttäjä saa halutessaan ilmoituksia tai videokuvaa päätelaitteeseensa. Joissakin systeemeissä saattaa olla myös muita ominaisuuksia, kuten lämpötilan ja ilmankosteuden ilmoittaminen (Williams, Terence J ja Immaculate 2019).

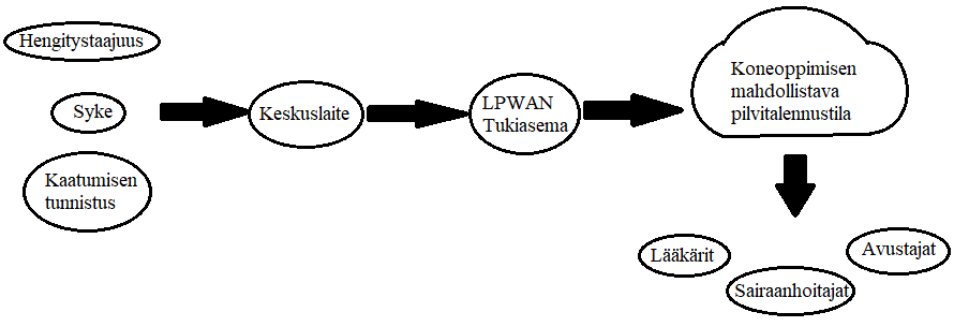
Esineiden internetiä voidaan myös hyödyntää infrastruktuurin ylläpitämisessä. IoT-laitteita käytetään mm. hyödyntämään energiatehokkuutta. Ihmisten energiakäytön ennalta-arvaamattomuuden vuoksi älyllisten laitteiden ja ohjelmien verkolla sähköverkon hallinta tulee helpommaksi (Albishi ym. 2017). Monia muitakin valvomiseen liittyviä tehtäviä voidaan helpottaa erillisten älylaitteiden avulla. Albishi ym. (2017) myös mainitsevat projektista, jossa Espanjalaisesta Santanderin kaupungista on tehty ns. ”älykaupunki”, jossa on tuhansia toisiinsa yhteydessä olevia sensoreita. Tätä testiä käydään yhdessä myös muidenkin kaupunkien kanssa.

Esineiden internetille on myös lääketieteellisiä käyttöjä. Tästä voidaan myös käyttää omaa termiä, esineiden lääketieteellinen internet (engl. *Internet of Medical Things*, tai *IoMT*). Väestön keski-iän nousun myötä myös monenlaiset terveyteen liittyvät riskit ovat lisääntyneet. Esineiden internetin hyödyntämistä pidetäänkin yhtenä ratkaisuna sairaanhoitojärjestelmien kohtaaman paineen helpottamiseksi. Suuri osa tutkimuksista liittyykin tiettyjen sairauksien, kuten diabetes, tarkkailuun IoT-laitteiden avulla (Baker, Xiang ja Atkinson 2017).

Baker, Xiang ja Atkinson (2017) esittävätkin artikkelissaan seuraavanlaisen mallin (kuvio 2.), joita eri sairaanhoitojärjestelmät voisivat käyttää tulevaisuudessa hyödyntäessään esinei-

den internetiä sairaanhoidon seuraamisen sujuvoittamiseksi:

1. Puettavat anturit ja keskuslaite
2. Lyhyen matkan kommunikaatio
3. Pitkän matkan kommunikaatio
4. Tietojen turvallinen tallettaminen, kuten pilvitallennuksen hyödyntäminen



Kuvio 2. IoMT esitetty malli (Baker, Xiang ja Atkinson 2017) mukaisesti tehtynä.

Puettavat anturit keräisivät datan (syke, kehonlämpö ym.), keskuslaite keräisi ne sekä lähettäisi ulkoiseen sijaintiin. Lyhyen matkan kommunikaatio olisi anturien ja päälaitteiden välillä. Kommunikaatiotapa ei saa aiheuttaa lisää terveysriskejä potilaalle, ja siinä tulisi tarvittaessa olla mahdollisimman matala viive. Pitkän matkan kommunikaatiolla tarkoitetaan keskuslaitteelta ulkoiseen tietokantaan lähetettävää dataa. Tärkeimpänä pitkän matkan kommunikaatiossa on turvallisuus sekä mahdollisten virheiden ja häirinnän esto. Baker, Xiang ja Atkinson (2017) pitävät pilvitallennustilaa turvallisimpana vaihtoehtona tietojen talletukselle. Erityistä huomiota tulisi kuitenkin kiinnittää siihen, että terveydehuollon ammattilaiset pääsevät käsiksi potilaiden tietoihin turvallisesti. He mainitsivat lisäksi koneoppimisen hyödyntämisen tietojen tutkimiseen suoraan pilvitallennustilasta.

Tuore esimerkki esineiden internetin hyödyntämisesta terveydenhuollossa on koronaepidemian aikaan tartuntojen seuraamisessa koronvilkun hyödyntäminen, joka älypuhelimen avulla ilmoitti mahdollisesta tartunnasta olemalla yhteydessä muihin älypuhelimiin. Koronavilkku ei lähettänyt muille päätelaitteille tarkkoja tietoja yksityisyyden suojan nojassa, ja sen käyttäminen oli täysin vapaaehtoista, joskin suositeltua.

3 Kyberturvallisuus

Digitaalisten laitteiden turvallisuudelle oli alkujaan useita eri termejä, kuten useimmille tuttu tietoturvallisuus. Vasta myöhemmässä vaiheessa alettiin käyttää termiä kyberturvallisuus, joka on sittemmin noussut suosiossa, samalla kun muiden termien suosio on laskussa (Schatz, Bashroush ja Wall 2017). Tässä luvussa määritellään, mitä kyberturvallisuus on, miten se eroaa tietoturvallisuudesta, sekä kyberturvallisuuteen liittyviä uhkia.

3.1 Kyberturvallisuuden määritelmä

Kyberturvallisuus tarkoitta kyberavaruuden (engl. *cyberspace*) turvallisuutta. Tietoturvallisuudella tarkoitetaan nimenomaan tiedon turvaamista, kun taas kyberturvallisuus kattaa koko kyberavaruuden. Solms ja Niekerk (2013) väittävätkin, että kyberturvallisuuden rajat ovat laajemmat, kuin tietoturvallisuuden, kun niiden virallista määritelmiä verrataan.

Tietoturvaan määrittyy kaikki tietoon liittyvät asiat, mukaan lukien systeemit ja laitteistot, jotka tallentavat, käyttävät ja lähettävät informaatiota (Whitman ja Mattord 2021). Samassa kirjassa mainitaan myös ns. CIA-kolmio/kolmikko (Luottamuksellisuus, ehjyys, saatavuus, engl. *Condfidentality, Integrity, Availability*), joka on alan standardiksi otettu malli tietoturvallisuuden ylläpitämisessä. CIA-kolmikkoa tosin pidetään jo jokseenkin puutteellisena mallina, joka vaatisi tarkentamista. Solms ja Niekerk (2013) haluavat myös lisätä, että tietoturvallisuus on muutakin kuin pelkkää teknologiaa, eikä pelkkien tuotteiden käyttäminen tietoturvallisuuden saavuttamiseksi ole tarpeeksi.

Kyberturvallisuus sisältää muutakin kuin tiedon turvaamista. Suuri osa kyberturvallisuuteen liittyvistä hyökkäyksistä saattaakin kohdistua tietoon, mutta on kuitenkin olemassa kyberuhkia, jotka eivät suoranaisesti liity informaatioon (Solms ja Niekerk 2013). Eräs heidän antamistaan esimerkeistä on seuraavanlainen: Älykodin laitteisiin kuuluu laitteita kodin turvajärjestelmistä televisioon. Internetin hyödyntämien laitteiden hallinnassa on kätevää, mutta se tuo myös mukanaan erilaisia turvallisuusriskejä. Laitteisiin käsiksi pääsemällä voidaan aiheuttaa vahinkoa, joko jotain lähes harmitonta, kuten tv käynnistelyä ja sammuttelua, aina turvajärjestelmien sammuttamiseen asti, jotta kodin pystyisi ryöstämään. Tällöin voidaan

väittää, ettei uhrin tietoihin ei ole kohdistunut vahinkoa, mutta uhrin muu omaisuus on ollut kyberrikoksen kohteena.

3.2 Kyberuhat

Seuraavassa taulukossa (Taulukko 1) on ENISAN (Euroopan unionin kyberturvallisuusvirasto) vuoden 2022 raportissa mainitut kahdeksan suurinta (kyber)uhkaa (“Enisa Threat Landscape 2022” 2022). Kyberuhkia on useita, joista jotkut kohdistuvat yksittäisiin henkilöihin ja joiden vahinko on suhteellisen pieni. Kyberuhat saattavat laajimmillaan kattaa kuitenkin koko yhteiskunnan kyberturvallisuuteen vaikuttavia hyökkäyksiä. Hyökkäykset infrastruktuuria ja logistiikkaa kohtaan voivat aiheuttaa suuriakin vahinkoja.

Kyberuhkia voidaan käyttää osana kybersotaa (vrt. ”fyysinen” sota). Muun muassa disinformaatio (ks. taulukko 1) on osa kybersotaa, jota esimerkiksi Venäjä on käyttänyt hyväkseen jo ennen heidän varsinaista hyökkäystään Ukrainaan (“Enisa Threat Landscape 2022” 2022).

Kyberuhkia voidaan käyttää myös eräänä aktivismin muotona, jota kutsutaan usein *Haktivismina*. Haktivistit hyödyntävät erilaisia hyökkäyksiä mm. web-palveluja kohtaan, saadakseen huomiota haluamaansa asiaan.

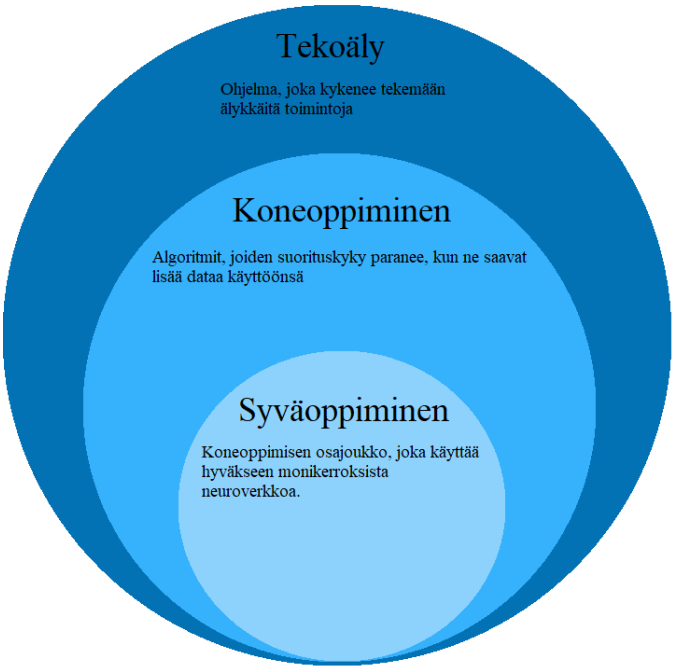
Enisan (“Enisa Threat Landscape 2022” 2022) raportissa mainitaan myös siitä, kuinka edistymiset koneoppimisessa, tekoälyssä sekä *deepfakeissä* on antanut hyökkääjille voimakkaita työkaluja disinformaation levittämiseen.

Taulukko 1. Kahdeksan suurinta kyberuhkaa

Uhka	Selitys
Kiristyohjelma	Kiristysohjelmassa hyökkääjä ottaa haltuunsa kohteen resursseja ja vaativat lunnaita, resurssien käyttökelvollisuuden palauttamista vastaan.
Haittaojelma	Haittaohjelmat ovat ohjelmia, jotka suorittavat luvattomia prosesseja ja aiheuttavat haittaa systeemin luottamuksellisuuteen, ehjyyteen tai saatavuuteen. Perinteisinä esimerkkeinä mm. virukset, troijalaiset ja vakoiluohjelmat.
Sosiaalinen manipulointi	Hyökkääjä manipuloi kohdetta sosiaalisesti hyödyntääkseen ihmisvirhettä, näin päästen käsiksi haluamiinsa tietoihin tai systeemeihin.
Uhka dataa kohtaan	Hyökkääjä yrittää saada luvattoman pääsyn dataan, sekä madollisesti häiritä systeemejä datan muokkaamisella. Hyökkäys dataa kohtaan sisältää käytännössä vain tietomurrot sekä tietojen levittäminen.
Palvelunesto-hyökkäys	Hyökkääjä häiritsee systeemien käytettävyyttä. Palvelunestohyökkäyksissä hyökkääjä ylikuormittaa palvelua jollain tavalla, samalla estäen pääsyn relevantteihin resursseihin.
Internetiin pääsyn estäminen	Hyökkääjä häiritsee suoraa pääsyä internetiin. Palvelunestohyökkäyksellä voidaan estää pääsy internetiin, mutta on ENISAN:n mainitsemissa uhissa määritelty erikseen.
Disinformaatio – Misinformaatio	Disinformaatio ja misinformaatio ovat hyvin lähellä toisiaan. Disinformaatio on tarkoituksellisesti harhaanjohtavaa tai väärää tietoa, kun taas misinformaatio tahallisesti tai tahattomasti levitettyä väärää tietoa.
Toimitusketjuun hyökkääminen	ENISAN oman määritelmän mukaan (“Enisa Threat Landscape for Supply Chain Attacks” 2021), toimitusketjuun kohdistuva hyökkäys koostuu ainakin kahdesta hyökkäyksestä. Jotta hyökkäystä voitaisiin kutsua toimitusketjuun hyökkäämiseksi, tulee molempien, toimittajan ja asiakkaan olla kohteita.

4 Tekoäly, koneoppiminen ja syväoppiminen

Tekoäly, ja varsinkin koneoppiminen, ovat ja tulevat tulevaisuudessakin olemaan tärkeä osa kyberturvallisuutta. Syväoppiminen on yksi koneoppimisen osajoukoista, joka on useilla aloilla muita koneoppimisen tekniikkoja tehokkaampi (kyberturvallisuus mukaan lukien) (Alzubaidi ym. 2021). Tässä luvussa käydään läpi nämä asiat läpi, joista koneoppiminen ja syväoppiminen hieman tarkemmin.



Kuvio 3. Tekoäly, koneoppiminen ja syväoppiminen (Alzubaidi ym. 2021) mukaisesti esitettynä.

4.1 Tekoäly

Tekoälyn juuret ylettyvät useiden vuosikymmenien taakse, on viimeaikaisimmat kehitykset alalla tehneet siitä tärkeän osan tulevaisuutta sekä uusia tutkimuskohteita (Barredo Arrieta ym. 2020). Tekoälyn ymmärtäminen onkin tärkeää, sillä yksi peloista sitä käyttäessä ja kehittäessä on juurikin se, että sen päätöksiä ei ymmärretä sekä niitä käytetään väärien syiden puitteessa. Selitettävissä olevan tekoälyn ideana on luoda uusia koneoppimisen malleja, joi-

ta ihmisten on helpompi ymmärtää ja luottaa, mutta ovat silti yhtä tehokkaita kuin nykyiset mallit (Barredo Arrieta ym. 2020).

Tekoälyä on käytetty hyväksi jossain määrin jo pitkään, mutta suurimmat edistymiset teknologiassa tapahtui vasta 2010-luvulla. Nykyään monet arkipäiväiset asiat saattavat käyttää tekoälyä hyväksiin, varsinkin jos ne ovat kytköksissä internetiin. Hakukoneet hyödyntävät sitä, että saisit mahdollisimman sopivia tuloksia hakusi perusteella, tai ainakin ensin annettuaan maksettujen mainosten tai sivustojen ehdotukset ensin. Jokainen haku ja sivulla käynti luultavasti myös tallentuu muistiin johonkin datakeskukseen, joiden perusteella tekoäly voi antaa juuri sinulle kohdennettuja mainoksia. Myös mm. shakissa tekoäly on ollut ihmistä parempia jo vuosikymmeniä, ja onkin tärkeässä roolissa nykyään pelien analysoinnissa. Kyberturvallisuudessa tekoälyä käytetään lähinnä koneoppimisen muodossa, joista enemmän tulevissa luvuissa (ks. luvut 4.2 ja 5.2)

4.2 Koneoppiminen ja syväoppiminen

Koneoppiminen sisältää algoritmeja, joiden tehokkuus parantuu, kun ne altistuvat kasvavalle määrälle dataa (Barredo Arrieta ym. 2020). Jordan ja Mitchell 2015 sanovat artikkelissaan, että (jo artikkelin julkaisuvuonna 2015) monet tekoälyjärjestelmien kehittäjät ymmärtävät kuinka järjestelmien kouluttaminen halutulla syöttö-tulos yhdistelmällä on helpompaa kuin itse näiden ohjelmointi.

Yleisin koneoppimisen muoto on ohjattu oppiminen (Lecun, Bengio ja Hinton 2015). Muita algoritmityyppejä ovat ohjaamaton oppiminen sekä vahvistusoppiminen. Ohjatussa oppimisessa opetusdatasta tiedetään valmiiksi haluttu tulos. Näiden perusteella tekoäly tekee ennustuksia uusista kyselyistä. Ohjaamattomassa oppimisessa tulosta ei varsinaisesti tiedetä valmiiksi, mutta datan rakenteesta on tiettyjä oletuksia (todennäköisyyksiä, kombinatoriikkaa ym.) (Jordan ja Mitchell 2015). Vahvistusoppiminen koneelle ei suoraan anneta oikeaa tulosta annetulle opetusdatalle, vaan pelkkä viittaus siihen, että tulos on oikea (Jordan ja Mitchell 2015). Voitaisiin siis sanoa, että kone ”palkitaan” oikeasta ratkaisusta.

Syväoppiminen on yksi koneoppimisen osajoukoista (ks. kuva 3), mikä käyttää hyödykseen monikerroksista neuroverkkoa (Lecun, Bengio ja Hinton 2015). Syväoppiminen on algorit-

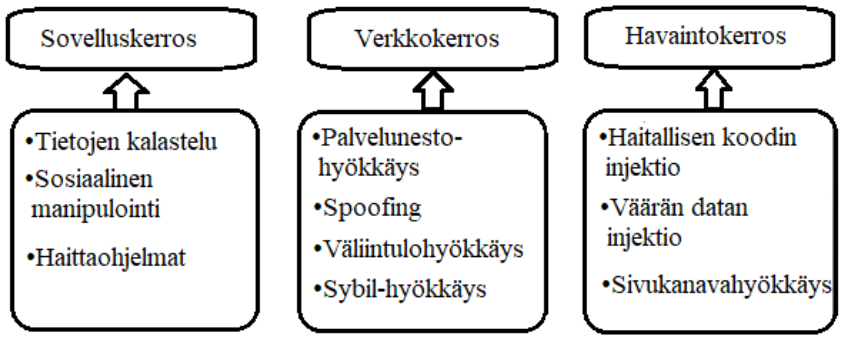
mityypiltään ohjattua oppimista, ja opetusdata saattaakin sisältää satoja miljoonia esimerkkejä, joiden avulla konetta opetetaan (Lecun, Bengio ja Hinton 2015). Lecun, Bengio ja Hinton 2015 myös väittävät, että syväoppimisen hyöty on siinä, kuinka sen hyödyntäminen vaatii melko vähän ihmisen omaa suunnittelua. Tällöin koneiden on helppo hyödyntää laskentatehon ja datan määrän kasvua.

5 Kyberturvallisuus esineiden internetissä

Esineiden internetin turvallisuus on yksi monesta IoT:n tämänhetkisistä haasteista. Turvallisuuteen vaikuttavat mm. vähäiset ja kelvottomat päivitykset, puuttuvat tehokkaat ja vahvat turvallisuusprotokollat sekä käyttäjien vähäinen tietämys (Tawalbeh ym. 2020). Tässä luvussa tutkitaan millaisia hyökkäyksiä IoT-laitteisiin kohdistuu, sekä miten koneoppimista hyödynnetään IoT-laitteiden turvallisuudessa sekä kyberturvallisuudessa yleisesti.

5.1 Esineiden internetiin kohdistuvat hyökkäykset

IoT-laitteisiin kohdistuvia hyökkäyksiä tapahtuu eri kerroksilla ja ne jaetaankin usein eri ryhmiin. Muun muassa Ghadeer (2018) on jakanut hyökkäykset seuraavanlaisesti: Fyysiset hyökkäykset, sovelluksiin kohdistuvat hyökkäykset sekä verkkoon kohdistuvat hyökkäykset (vrt. IoT:n kerrokset). Fyysiset hyökkäykset kohdistuvat IoT:n fyysiseen osaan, joka sisältää mm. sivukanavahyökkäyksen. Sovelluksiin kohdistuvat hyökkäykset koostuvat erilaisista haittaohjelmista, tietokoneviruksista ym. vastaavista. Verkkoon kohdistuvat hyökkäyksiin kuuluu mm. palvelunestohyökkäykset (aktiivinen hyökkäys) sekä kommunikaatiokanavien seuraaminen, kuuntelu ja muokkaaminen (passiivinen hyökkäys) (Ghadeer 2018).



Kuvio 4. Jotain yleisimpiä hyökkäyksiä IoT-laitteiden eri kerroksilla (Chen ym. 2022) mukaisesti esitettynä

Kuten kuviossa 4 vielä mainitaan, niin kuuluu sovelluskerrokseen myös sosiaalinen manipulointi. Tässä tutkielmassa keskitytään kuitenkin koneoppimisen hyödyntämiseen hyökkäyksien tunnistamisessa sekä estämisessä, joten sivuutetaan ihmisvirheitä koskevat hyökkäykset ainakin lähes kokonaan.

Eräs aiemmin mainitsematta jäänyt kerros on ns. reunakerros (engl. *edge layer, edge computing*). Reunalaskenta tapahtuu vielä erikseen pilven ja varsinaisten IoT-laitteiden välillä. Viiveen vähentämisen kannalta olisi hyvä, jos reunalaskenta tapahtuisi mahdollisimman lähellä IoT-laitteita. Joskus reunalaskentaa voidaan kutsu myös sumulaskennaksi (engl. *fog computing*, mutta joissain tapauksissa sumulaskentakin on vielä erillinen kerros reunalaskennan ja pilven välillä. Reunakerrokseen kohdistuvista hyökkäyksistä suurin osa on sivukanavahyökkäyksiä (Meneghello ym. 2019). Muita heidän mainitsemia hyökkäyksiä on mm. laitteistoon kohdistuvat troijalaiset sekä palvelunestohyökkäykset.

5.2 Koneoppiminen mukana kyberturvallisuudessa

Koneoppimisen kautta kyberturva ylläpitävät sovellukset voivat oppia tunnistamaan hyökkäystavat nopeammin ja tehokkaammin. Koneoppimisen tekniikkoja käytetäänkin jo laajasti eri tunkeilijoiden havaitsemisjärjestelmien (engl. *intrusion detection system, IDS*) kehittämisessä (Vinayakumar ym. 2019). Hyökkääjät kohdistavat hyökkäyksensä yhä useammin koneoppimisen malleja kohtaan (ks. luku 3.2).

Diro ja Chilamkurti (2018) kertovatkin, että päivittäin tapahtuu tuhansia nollapäivähaavoittuvuuksia hyödyntäviä hyökkäyksiä (engl. *zero-day vulnerability/attack*), juuri esineiden internetin vuoksi luotujen uusien protokollien myötä (lisää luvussa 5.3). He myös jatkavat, että nämä hyökkäykset ovat yleensä pieniä muokkauksia aiemmista tunnetuista hyökkäyksistä, jonka vuoksi perinteisillä koneoppimista hyödyntävillä järjestelmillä on vaikeuksia havaita näitä hyökkäyksiä. He vielä lisäävät, että juuri syväoppimista hyödyntävät järjestelmät ovat olleet varsin tehokkaita pienempiäkin muutoksia vastaan.

Kone- ja syväoppimisen hyöty kyberturvallisuudessa on siis siinä, kuinka ne (varsinkin syväoppiminen) pystyy ennustamaan tulevia hyökkäyksiä. Perinteisesti ihmiset ovat manuaalisesti tutkineet lokitiedostoja ja päivittäneet IDS:iä tarpeen mukaan (Vinayakumar ym. 2019).

Tämä metodi on tarkka juuri tunnettujen hyökkäysten kohdalla, mutta tuntemattomien hyökkäysten kohdalla lähes täysin hyödytöntä. Juuri tässä kohtaa koneoppiminen astuisi kuvaan. Väittäisin kuitenkin artikkeleiden ja muiden lähteiden perusteella, että vaikka koneoppiminen ja tekoäly yleensä on ottanutkin viime aikoina suuria askeleita kehityksessä, eivät ne vielä ole tarpeeksi hyviä kaikissa tapauksissa, ja vaativatkin vielä ihmisen valvontaa. Kuitenkin koneoppimisen hyödyt ovat selvät, sekä varmasti paranee jatkuvasti.

5.3 Hyödyntäminen IoT-laitteissa

Koneoppimisen myötä turvaa ylläpitävät sovellukset voivat olla tehokkaampia, sillä ihmisen ei tarvitse itse päivittää järjestelmiä jokaista uuttaa hyökkäystä vastaan. Toivon mukaan koneoppimisen ennusteet pystyisivät estämään ainakin suurimman osan hyökkäyksistä.

Diro ja Chilamkurti (2018) kertovatkin, että IoT-laitteiden tuomien hyötyjen vuoksi niiden kasvun suuri määrä aiheuttaa hankaluuksia kyberturvallisuuden kannalta, sillä tätä ylläpitävät laitteet ovat lähes aina jäljessä. He myös mainitsevat, että koska IoT on radikaalisti erilainen perinteisitä järjestelmistä sillä sen vaatimat palvelut ovat erityisiä, joita pelkkä keskitetty pilvipalvelu ei voi tyydyttää. Tässä aiemmin mainittu reuna/sumulaskenta tuleekin käyttöön eräänlaisena jatkeena perinteisille pilvipalveluille. Sumulaskennan avulla laskentateho voidaan ulkoistaa varsinaisilta dataa keräävіltä laitteilta verkon "reunalle", ja datan varsinainen säilytys voidaan jättää pilvipalveluille. Näin viive pysyy matalana ja datan käsittely on sekä turvallisempaa että nopeampaa.

Diro ja Chilamkurti (2018) myös kertovat mm. sumulaskennassa käytetyistä hyökkäystentunnistusrakenteista, joita on kaksi: Tunnisteisiin perustuva hyökkäyksen tunnistus sekä poikkeuksiin perustuva tunnistus. Tunnisteisiin perustuva hyökkäysten tunnistus vertaa tietoliikennettä jo tunnettuihin hyökkäyksiin. Tätä rakennetta pidetään hyvin tarkkana, mutta se ei pysty tunnistamaan uusia hyökkäyksiä. Poikkeuksiin perustuva tunnistus taas tunnistaa uudet hyökkäykset mutta se ei ole kovin tarkka. He myös mainitsevat, että molemmissa rakenteissa on käytetty hyväksi koneoppimista.

Palvelunestohyökkäyksiinkin vastaus löytyy pilvipalveluiden kautta. Niiden suuren kaistanleveyden myötä hyökkäyksiä ei välttämättä ole kovin suurta vaikutusta, vaikka IoT-laitteissa

olisikin haitallinen ohjelma. Tietysti optimaalisessa tilanteessa ohjelma ja sitä kautta bottiverkon leviämine saadaan estettyä jo reuna/sumulaskennan vaiheessa. Näissä tapauksissa koneoppiminen tulee taas esille, sillä hyökkääjät yrittävät jatkuvasti päivittää haittaohjelmiaan sekä etsiä mahdollisia haavoittuvuuksia. Väittäisin myös, että koneoppimista voidaan myös ylipäänsä hyödyntää palvelunestohyökkäyksien tunnistamisessa jopa pilvipalveluiden tasolla.

6 Yhteenveto

Väittäisin, että koneoppimisella ja tekoälyllä tulee olemaan suuri vaikutus kyberturvallisuuden ja sitä kautta esineiden internetin tulevaisuuteen. Esineiden internetissä on vielä tälläkin hetkelle paljon vajaavaisuutta kyberturvallisuuden puolella, ja mm. koneoppiminen voi auttaa paikkaamaan näitä reikiä.

Eniten tätä aihetta tutkiessa tuli vastaan reuna- ja sumulaskenta hyödyntäminen. Reunalaskennassa laskentateho siirtyisi matalatehoisilta IoT-laitteilta erilliseen mutta mahdollisimman läheiseen keskukseen. Tällä tavoin viive saataisiin pidettyä mahdollisimman matalana, mutta itse datan tallennus voitaisiin jättää vielä isommille ja pilvitallennukseen ja -laskentaan tarkoitetuille keskuksille. Reunalaskennan avulla koneoppimista voidaan hyödyntää paremmin, sillä hyökkäyksiin voidaan vastata nopeammin sekä tehokkaammin, kuin pelkästään IoT-laitteiden ja pilvipalveluiden avulla.

Vanhojen laitteiden päivittäminen on myös eräs haasteista esineiden internetin kyberturvallisuuden ylläpitämisessä. Tämä aihe pitkälti sivuutettiin aiheissa. Väittäisin että tämä johtuu siitä, että siihen ei juurikaan ole muuta vastausta kuin laitteiden päivittäminen, joka usein saattaa vaatia kokonaan uusien laitteiden hankkimista. Tämä siis johtaisi kuluihin, joita yritykset eivät välttämättä halua. Tosin reuna- ja pilvilaskenta voiva olla tähänkin vastaus, mikäli laitteet ovat yhteydessä tällaisiin.

Lähteet

Albishi, Saad, Ben Soh, Azmat Ullah ja Fahad Algarni. 2017. “Challenges and Solutions for Applications and Technologies in the Internet of Things”, 124:608–614. https://doi.org/10.1016/j.procs.2017.12.196.

Ali, Rao Faizan, Amgad Muneer, P.D.D. Dominic, Shakirah Mohd Taib ja Ebrahim A. A. Ghaleb. 2021. “Internet of Things (IoT) Security Challenges and Solutions: A Systematic Literature Review”. *Communications in Computer and Information Science* 1487 CCIS:128–154. https://doi.org/10.1007/978-981-16-8059-5_9.

Alzubaidi, Laith, Jinglan Zhang, Amjad J. Humaidi, Ayad Al-Dujaili, Ye Duan, Omran Al-Shamma, J. Santamaría, Mohammed A. Fadhel, Muthana Al-Amidie ja Laith Farhan. 2021. “Review of deep learning: concepts, CNN architectures, challenges, applications, future directions”. *Journal of Big Data* 8 (1). https://doi.org/10.1186/s40537-021-00444-8.

Ashton, Kevin. 2009. “That ‘internet of things’ thing”. *RFiD Journal* 22:97–114.

Baker, Stephanie B., Wei Xiang ja Ian Atkinson. 2017. “Internet of Things for Smart Healthcare: Technologies, Challenges, and Opportunities”. *IEEE Access* 5:26521–26544. https://doi.org/10.1109/ACCESS.2017.2775180.

Barredo Arrieta, Alejandro, Natalia Díaz-Rodríguez, Javier Del Ser, Adrien Bennetot, Siham Tabik, Alberto Barbado, Salvador Garcia ym. 2020. “Explainable Artificial Intelligence (XAI): Concepts, taxonomies, opportunities and challenges toward responsible AI”. *Information Fusion* 58:82–115. https://doi.org/10.1016/j.inffus.2019.12.012.

Chen, Zhiyan, Jinxin Liu, Yu Shen, Murat Simsek, Burak Kantarci, Hussein T. Mouftah ja Petar Djukic. 2022. “Machine Learning-Enabled IoT Security: Open Issues and Challenges under Advanced Persistent Threats”. *ACM Computing Surveys* 55 (5): 12–45. https://doi.org/10.1145/3530812.

“Cisco Annual Internet Report”. 2020, https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.pdf.

Diro, Abebe Abeshu, ja Naveen Chilamkurti. 2018. “Distributed attack detection scheme using deep learning approach for Internet of Things”. *Future Generation Computer Systems* 82:761–768. https://doi.org/10.1016/j.future.2017.08.043.

“Enisa Threat Landscape 2022”. 2022, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022.

“Enisa Threat Landscape for Supply Chain Attacks”. 2021, https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks.

Ghadeer, Hoda. 2018. “Cybersecurity Issues in Internet of Things and Countermeasures”. Teoksessa *2018 IEEE International Conference on Industrial Internet (ICII),* 195–201. https://doi.org/10.1109/ICII.2018.00037.

Jordan, M.I., ja T.M. Mitchell. 2015. “Machine learning: Trends, perspectives, and prospects”. *Science* 349 (6245): 255–260. https://doi.org/10.1126/science.aaa8415.

Lecun, Yann, Yoshua Bengio ja Geoffrey Hinton. 2015. “Deep learning”. *Nature* 521 (7553): 436–444. https://doi.org/10.1038/nature14539.

Meneghello, Francesca, Matteo Calore, Daniel Zucchetto, Michele Polese ja Andrea Zanella. 2019. “IoT: Internet of Threats? A Survey of Practical Security Vulnerabilities in Real IoT Devices”. *IEEE Internet of Things Journal* 6 (5): 8182–8201. https://doi.org/10.1109/JIOT.2019.2935189.

Schatz, Daniel, Rabih Bashroush ja Julie Wall. 2017. “Towards a More Representative Definition of Cyber Security”. *Journal of Digital Forensics* 12 (2). https://doi.org/10.15394/jdfsl.2017.1476.

Sethi, Pallavi, ja Smruti Sarangi. 2017. “Internet of Things: Architectures, Protocols, and Applications”. *Journal of Electrical and Computer Engineering* 2017:1–25. https://doi.org/10.1155/2017/9324035.

Solms, Rossouw von, ja Johan van Niekerk. 2013. “From information security to cyber security”. *Computers & Security* 38:97–102. https://doi.org/10.1016/j.cose.2013.04.004.

Tawalbeh, Lo'ai, Fadi Muheidat, Mais Tawalbeh ja Muhannad Quwaider. 2020. "IoT privacy and security: Challenges and solutions". *Applied Sciences (Switzerland)* 10 (12). https://doi.org/10.3390/app10124102.

Whitman, Michael E, ja Herbert J Mattord. 2021. *Principles of information security.* Cengage learning.

Williams, Vasanth, Sebastian Terence J ja Jude Immaculate. 2019. "Survey on internet of things based smart home", 460–464. https://doi.org/10.1109/ISS1.2019.8908112.

Vinayakumar, R., Mamoun Alazab, K.P. Soman, Prabaharan Poornachandran, Ameer Al-Nemrat ja Sitalakshmi Venkatraman. 2019. "Deep Learning Approach for Intelligent Intrusion Detection System". *IEEE Access* 7:41525–41550. https://doi.org/10.1109/ACCESS.2019.2895334.

Zhou, Ian, Imran Makhdoom, Negin Shariati, Muhammad Ahmad Raza, Rasool Keshavarz, Justin Lipman, Mehran Abolhasan ja Abbas Jamalipour. 2021. "Internet of Things 2.0: Concepts, Applications, and Future Directions". *IEEE Access* 9:70961–71012. https://doi.org/10.1109/ACCESS.2021.3078549.