Mikael Herrala

YRITYKSEN TIETOTURVAN KEHITTÄMINEN TEKOÄLYN AVULLA

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2024

TIIVISTELMÄ

Herrala, Mikael
Yrityksen tietoturvan kehittäminen tekoälyn avulla
Jyväskylä: Jyväskylän yliopisto, 2023, 24 s.
Tietojärjestelmätiede, kandidaatin tutkielma
Ohjaaja(t): Clements, Kati

Tekoäly on yksi nykypäivän tutkituimmista teknologioista tehokkuutensa ja valtavan potentiaalinsa ansiosta. Tekoälyn kehitys on mahdollistanut sen hyödyntämisen useilla eri aloilla, minkä seurauksena yritykset ovat alkaneet hyödyntämään sitä myös tietoturvan kehittämisessä. Tämän kanditutkielman tarkoituksena on perehtyä tekoälyyn ja yrityksien tietoturvaan, sekä tarkastella tekoälyn mahdollisuuksia erityisesti yritysten tietoturvan kehittämisessä. Tutkielma toteutettiin kirjallisuuskatsauksena, ja tiedonhaussa pyrittiin käyttämään tunnettuja ja luotettavia tietokantoja. Tutkielman tutkimuskysymys on: ”Millä tavoin tekoälyä voidaan hyödyntää yrityksen tietoturvan kehittämisessä?” Tutkimus koostuu kolmesta pääluvusta. Ensimmäisessä käydään läpi tekoälyn määritelmää, muotoja ja historiaa. Toisessa luvussa tutustutaan tietoturvaan ja sen määritelmään. Kolmannessa pyritään vastaamaan tutkimuskysymykseen kahden ensimmäisen luvun pohjalta. Tutkielma nostaa esiin tekoälyteknologioiden mukanaan tuomat hyödyt, erityisesti yrityksien tietoturvan näkökulmasta. Tutkielman johtopäätöksenä voidaan todeta, että tekoälyä voidaan hyödyntää tietoturvan kehityksessä, ja sen rooli voidaan määritellä yrityksen tarpeiden mukaan. Mukautuvuus onkin tekoälyjärjestelmän suurin vahvuus. Tekoälyn käyttö ei kuitenkaan ole ongelmatonta, ja laaja-alainen tekoälyn hyödyntäminen edellyttää tekoälyteknologioiden jatkuvaa kehitystä.

Asiasanat: tekoäly, tietoturva, yritys, kehitys, koneoppiminen

ABSTRACT

Herrala, Mikael
Improving information security with artificial intelligence
Jyväskylä: University of Jyväskylä, 2023, 24 pp.
Information Systems, bachelor's degree
Supervisor(s): Clements, Kati

Artificial Intelligence (AI) is one of today's most researched technologies, thanks to its efficiency and great potential. The development of artificial intelligence has made it possible to use it in many different areas, because of which companies have also started to use it in the development of information security. The purpose of this thesis is to study AI and information security in enterprises, and to examine the potential of AI especially in the development of information security in enterprises. The thesis was made as a literature review, and the aim was to use well-known and reliable databases to search for information. The research question of the thesis is: "How can AI be used to improve information security in the enterprise?". The study consists of three main chapters. The first one reviews the definition, forms, and history of AI. The second chapter introduces security and its definition. The third seeks to answer the research question based on the first two chapters. The thesis highlights the benefits of AI technologies, especially from the perspective of enterprise security. The thesis concludes that AI can be used in the development of information security and its role can be defined according to the needs of the company. In fact, adaptability is the main strength of an AI system. However, the use of AI is not without its problems, and the widespread use of AI requires continuous development of AI technologies.

Keywords: artificial intelligence, information security, enterprise, development, machine learning

KUVIOT

TAULUKOT

SISÄLLYS

1 JOHDANTO

Tässä kandidaatin tutkielmassa tutkitaan, miten yritysten tietoturvaa voidaan kehittää tekoälyä hyödyntäen. Tutkielman tavoitteena on esitellä tekoälyn luomia keinoja, joita käyttämällä yritykset kykenevät kehittämään tietoturvaansa. Tutkielma koostuu kolmesta pääkappaleesta: tekoälystä, tietoturvasta ja tutkimuskysymykseen vastaavasta kappaleesta, joka käy läpi tekoälyn synnyttämiä keinoja yrityksen tietoturvan kehittämiseen.

Tutkielman ensimmäisessä osassa määritellään tekoäly sekä käydään läpi sen historiaa ja osa-alueita. Ailiston ym. (2018) mukaan tekoäly ei ole yksi kokonaisuus vaan kokoelma erilaisia teknologioita ja sovelluksia. Tekoälyn määrittely on haastavaa sen monikäyttöisyyden ja käsitteen laajuuden vuoksi (Haenlein & Kaplan, 2019). Tutkielmassa tekoälyn katsotaan olevan tietojärjestelmä tai ohjelma, joka kykenee oppimaan ja mukautumaan (Ailisto ym., 2018). Tekoälytutkimus kehittyy jatkuvasti, mikä hankaloittaa tekoälyn määrittelyä ja rajaamista tiettyihin raameihin.

Tutkielman toisessa osassa käsitellään tietoturvaa, joka tarkoittaa tiedon saatavuuden, luottamuksellisuuden ja eheyden ylläpitoa (Samonas & Coss, 2014). Tietoturva on käsitteenä laaja, mutta sen tavoite on selkeä: tietoturvan tarkoituksena on taata yrityksen toiminnan jatkuvuus, sekä minimoida vahingot, joita tietoturvaongelmat voivat aiheuttaa (Von Solms & Van Niekerk, 2013).

Tutkielman kolmannessa osassa kerrotaan, miksi tekoäly voi olla ratkaisu nykypäivän tietoturvahaasteisiin. Digitalisaation ja verkkoteknologian kehittyessä yritysten tietoturvahaasteet kasvavat. Perinteiset ratkaisutavat eivät aina riitä, ja yritysten on käytettävä uusia teknologioita, kuten tekoälyä, tietoturvan parantamiseksi ja riskien hallitsemiseksi. Tekoäly päivittää itseään automaattisesti ja kehittyy ajan myötä, minkä vuoksi se voi olla tehokas ratkaisu myös tietoturvan kehityksessä. (Dhingra ym., 2016; Wang ym., 2023).

Tietoturva on ollut olemassa käytännössä yhtä kauan kuin tietokoneita on ollut käytössä. Jatkuva kilpajuoksu tietojärjestelmien puolustuksen ja hyökkääjien kanssa on ollut käynnissä vuosikymmeniä. Tekoälyn voisi luulla olevan ratkaisu tähän; voidaanko tekoälyn avulla viimeinkin rakentaa tietojärjestelmille

puolustus, jota ei voi murtaa? Valitettavasti tekoälyä on mahdollista hyödyntää myös hyökkäykseen, minkä vuoksi parhaan puolustuksen – sekä hyökkäyksen, saa parhaan tekoälyn omistama taho. Tekoälyn hyödyntämistä yritysten tietoturvan kehityksessä ei ole vielä tutkittu kovinkaan paljon: lisätutkimuksen tarve on valtava. Tekoälyn potentiaali tietoturvan kehittämisessä on suuri, ja sen avulla on mahdollisuus ottaa harppaus kohti turvallisempaa tietoa. Tutkielman tarkoituksena onkin selvittää, miten tekoälyn eri muotoja voidaan käyttää tiedon turvaamisessa. Tutkielman tutkimuskysymys on seuraava:

- Millä tavoin tekoälyä voidaan hyödyntää yrityksen tietoturvan kehittämisessä?

Tutkielma on toteutettu kirjallisuuskatsauksena. Aineiston keräämisessä on käytetty monia eri tietokantoja: JYKDOK-kirjastoa, ACM Digital Librarya, IEEE-Xplore-kirjastoa, Google Scholar- hakupalvelua sekä Scopus- tietokantaa. Lähdekirjallisuuden hakusanoina on käytetty seuraavia hakusanoja ja niiden yhdistelmiä: “artificial intelligence”, “AI”, “information security”, “enterprise”, “tietoturva”, “tekoäly”, “security”, “machine learning”, “deep learning” ja “neural networks”. Tutkielman lähteet on pyritty pitämään laadukkaina ja vertaisarvioituina, minkä lisäksi käytettyihin lähteisiin on viitattu muissa tutkimuksissa tuoden niille uskottavuutta. Tutkielman suurin rajoite oli yksityiskohtaisen tiedon hankinta tekoälyn hyödyntämiselle tietoturvan kehittämisessä. Aiheesta on julkisesti saatavilla suhteellisen vähän tutkittua tietoa, minkä vuoksi asiaa on tärkeää tutkia myös jatkossa.

2 TEKOÄLY

Tämän luvun tarkoituksena on määritellä tekoälyä, käydä läpi sen historiaa, tarkastella tekoälyn eri muotoja sekä tulevaisuuden näkymiä. Ensimmäisessä alaluvussa pohditaan tekoälyn määrittelyä. Toisessa alaluvussa käydään läpi tekoälyn historiaa. Kolmannessa alaluvussa käydään läpi tekoälyn osa-alueita, kuten koneoppimista ja siihen liittyvää syväoppimista. Neljännessä alaluvussa tarkoitus on nostaa esiin tekoälyn tulevaisuuden näkymät ja potentiaali.

2.1 Tekoälyn määrittely

Tekoäly on käsitteenä laaja ja moniulotteinen. Se ei ole yksi teknologia, vaan nimikkeen alle kuuluu laaja kirjo erilaisia menetelmiä, teknologioita, sovelluksia ja tutkimussuuntia (Ailisto ym., 2018). Ailisto ym. (2018) määrittelee tekoälyn Russelia ja Norvigia (2014) mukaillen seuraavasti: ”Tekoälyn avulla koneet, laitteet, ohjelmat, järjestelmät ja palvelut voivat toimia tehtävän ja tilanteen mukaisesti järkevällä tavalla.” Michael Haenlein ja Andreas Kaplan (2019) määrittelevät tekoälyn järjestelmän kyvyksi tulkita ulkoista dataa oikein, oppia siitä, ja käyttää näitä oppeja tiettyjen tavoitteiden ja tehtävien saavuttamiseen joustavalla mukauttamisella. Kaikki mainitut määritelmät ovat hyvin samankaltaisia keskenään, mistä voidaan päätellä, että mukautumiskyky on tärkeässä roolissa tekoälyn toiminnassa.

Tekoälyn kehitys voidaan jakaa karkeasti kolmeen kehitysvaiheeseen: kapeaan tekoälyyn, johon kaikki tämän hetken tekoälyt kuuluvat, yleiseen tekoälyyn ja superälyyn (Haenlein & Kaplan, 2019).

2.2 Tekoälyn historia

Älykäs kone on ollut filosofisten pohdintojen aiheena jo vuosisatojen ajan. Aikojen saatossa tekoälyyn liittyviä pohdintoja ovat esittäneet esimerkiksi René Descartes, Wilhelm Leibniz, ja Blaise Pascal. Descartesin pohdinnat keskittyivät enemmänkin metaforaan mekaanisesta miehestä, kuin varsinaiseen mahdollisuuteen sen olemassaolosta. Leibniz ja Pascal sunnittelivat laskimen tapaisen esineen, mutta eivät koskaan väittäneet, että koneet voisivat jonain päivänä ajatella (Buchanan, 2006). Ensimmäisen laskimen rakensi lopulta saksalainen tiedemies Wilhelm Shickard noin vuonna 1623 (Russel & Norvig, 2014).

On vaikea löytää tarkkaa ajankohtaa tekoälyn (AI) synnylle, mutta ensimmäisiä viitteitä tekoälyn synnystä löytyy vuodelta 1942, jolloin Isaac Asimov

julkaisi lyhyen teoksen: Runaroundin, jossa kehitetään älykäs robotti. Robotille annetaan teoksessa kolme lakia: (1) Robotti ei saa vahingoittaa ihmistä, eikä se saa päästää ihmistä vahingoittumaan. (2) Robotin pitää totella ihmisiltä saatuja käskyjä, jos niiden toteuttaminen ei riko ensimmäistä sääntöä. (3) Robotin pitää suojella omaa selviytymistään niin kauan, kun se ei riko sääntöjä 1 ja 2 (Haenlein & Kaplan, 2019).

Tekoälyn kehitys mahdollistui monien eri tieteenalojen kehittymisen myötä. Esimerkiksi biologian, fysiikan ja psykologian tutkimuksen kehittyminen antoivat tekoälytutkimukselle mahdollisuuden onnistua. Alan Turing julkaisi vuonna 1950 Mind -lehdessä tutkimuksen, jota pidetään yleisesti alkusysäyksenä tekoälytutkimukselle. Tutkimus pohtii ohjelmoinnin mahdollisuuksia saada tietokone käyttäytymään älykkäästi, ja sisältää kuuluisan Turingin testin. (Buchanan, 2006)

Ensimmäisen oppimista hyödyntävän ohjelman kirjoitti Anthony Oettinger. Ohjelma oli nimeltään ”response learning programme”, tai ”shopping programme” ja se tehtiin vuonna 1951. Ohjelma jäljitteli lapsen käyttäytymistä kaupassa käymisessä (Shinde ja Shah 2018). Tekoälyä ei ollut vielä 1951 vielä määritelty, eikä sillä ollut yleisesti käytössä olevaa termiä. Vasta vuonna 1956 John McCarthy käytti ensimmäistä kertaa termiä ”artificial intelligence” eli tekoälyä kuvailemaan tiedettä ja suunnittelua, jossa pyritään rakentamaan älykkäitä koneita (Kaul ym., 2020).

Seppo Linnainmaa esitteli vuonna 1970 mahdollisesti ensimmäisen ”taaksepäinlevitys” algoritmin. Vuonna 1981 Paul Werbos yhdisti taaksepäinlevitysalgoritmin neuroverkkoihin, ja sai aikaan monikerroksisen neuroverkon.

Iso harppaus tekoälyn kehitykselle tapahtui vuonna 1995, kun Vapnik ja Cortes kehittivät tukivektorikoneen (SVM). Kehityksen myötä koneoppimisen tutkijat jakautuivat kahteen eri ryhmään, neuroverkkojen ja tukivektorikoneen tutkijoihin (Shinde ja Shah 2018).

Yoav Freund ja Robert Schapire kehittivät vuonna 1997 algoritmin, joka hyödynsi heikkojen luokittelijoiden tehostettua kokonaisuutta, nimeltään Adaptive Boost (AdaBoost). Leo Breiman tutki Adaboostin mahdollisuuksia, ja rakensi sen pohjalta tutkimuksensa Random Forest -algoritmista, joka on vankempi versio Adaboostista (Shinde ja Shah, 2018).

Vuonna 2010 tekoälyn kehitys räjähti kolmen mahdollistavan tekijän ansiosta: Massadatan saatavuus helpottui, koneoppiminen kehittyi, ja tietokoneiden tehokkuus nousi (Sayler, 2020).

Keinotekoinen neuraaliverkko (ANN, artificial neural network), nosti syväoppimisen taas kiinnostuksen kohteeksi vuonna 2015, kun AlphaGo, Googlen kehittämä tekoäly voitti lajin maailmanmestarin Go-lautapelissä. Go on huomattavasti monimutkaisempi lautapeli kuin shakki, ja oli pitkään kuviteltu, ettei tekoäly voittaisi ihmistä koskaan kyseisessä pelissä (Haenlein & Kaplan, 2019).

2.3 Tekoälyn muotoja

Edellisen vuosikymmenen aikana tekoälystä on tullut suosittu aihealue tiedeyhteisön sisällä ja ulkopuolella. Tekoälyn tutkimus on lisääntynyt kahdessa aallossa. Ensin vuosina 2004–2007 tieteellisten julkaisujen määrä nousi 30 000:sta 60 000:een. Vuonna 2018 julkaistiin jo 80 000 tutkimusta vuodessa (Ailisto ym., 2018). Tekoälystä julkaistaan jatkuvasti enemmän artikkeleita, joissa keskitytään koneoppimiseen, syväoppimiseen ja tekoälyyn. Termien käytössä ja ymmärtämisessä on kuitenkin vielä parantamisen varaa, ja tässä kappaleessa keskitytään tekoälyn eri muotoihin ja niiden vahvuuksiin (Choi ym., 2020).

Tekoäly on ala, joka keskittyy älyllisten tehtävien automatisointiin, jotka normaalisti suoritetaan ihmisten toimesta. Koneoppiminen ja syväoppiminen ovat tekoälyn muotoja, joiden avulla yritetään päästä samaan lopputulokseen. Eri menetelmillä on eri vahvuusalueita, jotka tiedostamalla voidaan valita oikea menetelmä tietyn asian suorittamiseen. (Choi ym., 2020)

Koneoppiminen on tekoälyn osa-alue ja syväoppiminen on koneoppimisen osa-alue. Koneoppiminen on kehittynyt valtavasti edellisten vuosikymmenten aikana. (Shinde ja Shah, 2018)

2.3.1 Koneoppiminen

Ailiston ym. (2018) mukaan koneoppiminen on tietokonetekniikan osa-alue, joka käyttää tilastotieteen menetelmiä antaakseen tietokoneelle kyvyn oppia datasta, ilman yksityiskohtaista ohjelmointia. Koneoppiminen on alue, joka yhdistää tekoälyn, tietojenkäsittelytieteen ja data-analytiikan menetelmiä. Myös Kaul ym. (2020) kertoo tutkimuksessaan, että koneoppimisessa sovelletaan tilanteeseen sopivaa algoritmia luomaan malleja, joita voidaan käyttää tietyn tilanteen analysointiin. Kone voi siten oppia, ja soveltaa oppimiaan asioita vastaavanlaisiin tilanteisiin tulevaisuudessa.

Koneoppiminen on iso osa tekoälyä, mutta tekoäly on laajempi käsite kuin pelkkä koneoppiminen, koska sillä on myös kyky ymmärtää dataa, sekä käyttää, liikuttaa ja ohjata sitä tarpeen mukaan. Esimerkiksi luonnollisten kielten käsittelyssä ja kuvan- tai äänentunnistuksessa hyödynnetään näitä ominaisuuksia. (Haenlein & Kaplan, 2019). Koneoppiminen sisältää kolme yleisesti määriteltyä osa-aluetta: ohjattu oppiminen, ohjaamaton oppiminen, ja vahvistusoppiminen (Russell & Norvig, 2016).

2.3.2 Syväoppiminen

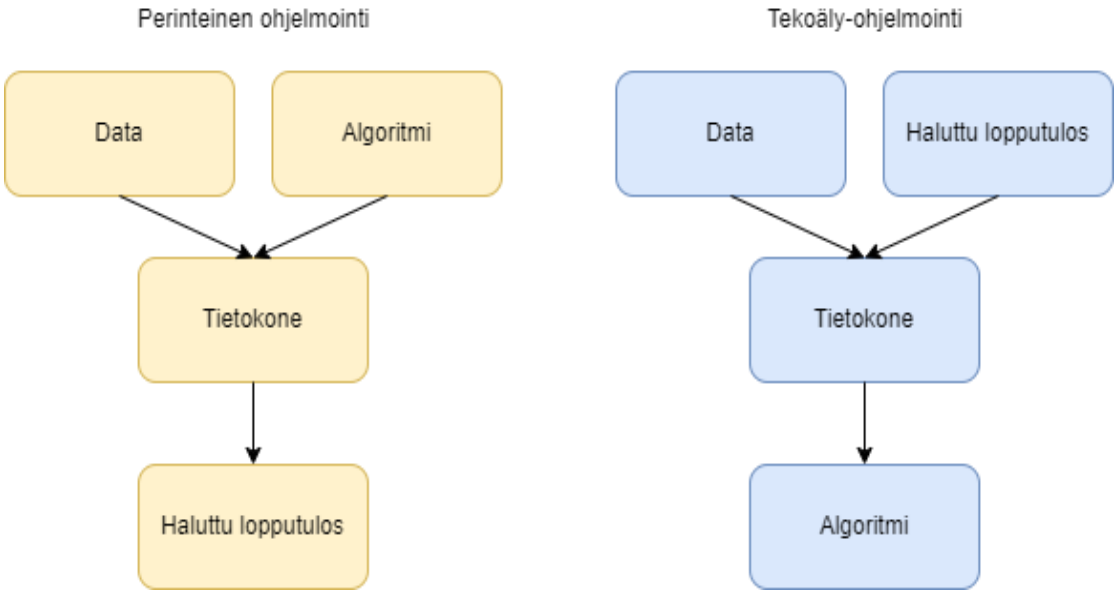
Syväoppiminen tarkoittaa tekoälyteknologioita, jotka hyödyntävät useista käsittelykerroksista koostuvia neuroverkkoja. Nämä menetelmät ovat parantaneet dramaattisesti puheentunnistuksen, kuvien tunnistuksen, ja monien muiden alojen, kuten lääkekehityksen huippua. Syväoppiminen löytää suurista tietojoukoista rakenteen käyttämällä takaisinlevitys -algoritmia osoittamaan, kuinka koneen tulisi muuttaa sisäisiä parametrejaan, joita käytetään kunkin kerroksen lopputuloksen laskemiseen edellisen kerroksen tuottamasta tuloksesta. (LeCun, 2015)

Syväoppiminen on koneoppimisen osa-alue. 'Syvä' viittaa neuroverkon kerroksiin: syvä neuroverkko sisältää vähintään kaksi piilotettua tasoa, kun taas ohut verkko sisältää vain yhden (Shinde & Shah, 2018). Syväoppimisen nopea kehitys on johtanut tekoälyyn liittyvien odotuksien nousuun. Neuroverkot hyötyvät laskentatehon ja saatavilla olevan datan määrän kasvusta, minkä vuoksi niillä voi olla tulevaisuudessa iso rooli tekoälyn kehityksessä (LeCun ym., 2015). Shinden ja Shahin vuonna 2018 julkaistussa tutkimuksessa kerrotaan, että syväoppiminen voi olla ratkaisu nousseisiin odotuksiin, koska ne kykenevät oppimaan suurista määristä dataa, sekä monista eri lähteistä saadusta datasta.

Tärkein ero neuroverkkojen ja tilastollisten lähestymistapojen välillä on se, että neuroverkot eivät tee oletuksia datan tilastollisesta jakaumasta tai ominaisuuksista, ja siksi ne ovat yleensä hyödyllisempiä käytännön tilanteissa. Neuroverkot ovat myös luonnostaan epälineaarinen lähestymistapa, mikä antaa niille paljon tarkkuutta monimutkaisten tietomallien mallintamisessa (Smith & Gupta, 2000).

2.3.3 Perinteisen ohjelmoinnin ja tekoälyohjelmoinnin erot

Perinteisessä ohjelmoinnissa algoritmi koodataan tiettyjä ominaisuuksia hyödyntäen. Koneoppimisessa käytetään dataa oppimiseen, ja rakennetaan sen avulla algoritmi, jossa on erilaisia ominaisuuksia ja painotuksia kuin perinteisessä ohjelmoinnissa (Kuvio 1), (Choi ym., 2020). Perinteisessä ohjelmoinnissa järjestelmän kehittäjät määrittelevät ohjelmalle säännöt, miten toimia eri tilanteissa. Koneoppimisessa ajatuksena on se, että kone oppii sen saadusta informaatiosta. Koneoppimisen tekoälymallit opetetaan toimimaan oikein; isolla joukolla esimerkkejä sisältävällä datalla, tai palkitsemalla sen oppimaan oikeaan suuntaan (Vartiainen ym., 2021; Russell & Norvig, 2016).



KUVIO 1 (mukaillen, Choi ym., 2020)

2.4 Tekoälyn tulevaisuus

Tekoälyn potentiaali on valtava: Wired-lehden perustajan Kevin Kelleyn mukaan: ”Tekoäly tulee elävöittämään elottomia esineitä yhtä paljon kuin sähkö teki, yli vuosisata sitten. Kaikki mitä aikaisemmin sähköistimme, tulevat tiedostamaan ympäröivän maailman.” (Sayler, 2022). Hyvä esimerkki tekoälyn potentiaalista löytyy lääketieteestä. Algoritmit ovat jo nyt parempia kuin radiologit havaitsemaan pahanlaatuisia kasvaimia, ja ohjaavat tutkijoita kohorttien muodostamisessa kliinisiä tutkimuksia varten (Davenport & Kalakota, 2019).

Wilsonin ym. (2018) mukaan tekoäly tulee korvaamaan suuren määrän työpaikkoja tulevaisuudessa, tekoälyteknologioiden kehittyessä entistä paremmiksi. Tekoälyn kehittyminen tulee kuitenkin myös luomaan uusia, ennennäkemättömiä työmahdollisuuksia. Wilson ym. (2018) viittaavat Accenture PLC:n tutkimukseen, joka osoittaa, että yli tuhannen suuren yrityksen keskuudessa, jotka ovat jo käyttäneet tai testanneet tekoälyä ja koneoppimista, on syntymässä uudenlaisia, ennennäkemättömiä työtehtäviä. Nämä tehtävät eivät korvaa vanhoja, vaan ne ovat täysin uudenlaisia ja vaativat taitoja ja koulutusta, joita aikaisemmin ei ole ollut.

Tekoälyllä on myös mahdollisuus kehittää myös tietoturva ennen näkemättömälle tasolle. Sillä on kyky käsitellä nopeasti suuria määriä dataa, erottaa poikkeamat ja automatisoida toimenpiteet tietoturvaongelmiin, minkä vuoksi sen potentiaali myös tietoturvan kehityksessä on valtava (Mughal, 2018). Tekoälyn

kehittäminen ei kuitenkaan ole ongelmatonta. Hu ym. (2021) käyvät tutkimuksessaan läpi tekoälyn tekoälyjärjestelmien ongelmia, ja ratkaisuja. Suurin haaste on datan keräysvaiheessa; digitaalinen data voi sisältää vääristynyttä tai jopa täysin väärää tietoa, minkä lisäksi tietokanta on voinut altistua hyökkäykselle. Tekoäly on todella haavoittuvaisessa asemassa, jos sen käyttämä harjoitusdata on vääristynyttä.

3 TIETOTURVA

Tämän luvun tavoitteena on käydä läpi tietoturvan perusteet, sekä tietoturvan tavoitteita. Ensimmäinen alaluku käsittelee tietoturvan perusteita ja yleisimpiä käsitteitä. Toisen alaluvun tarkoituksena on avata, mitä tietoturvan ylläpitämisellä pyritään saavuttamaan.

3.1 Tietoturvan perusteet

Tietoturva on yleiskäsite hallinnollisille ja teknisille toimille, joilla varmistetaan tiedon luottamuksellisuus, eheys ja käytettävyys. Luottamuksellisuus tarkoittaa, että tiedot ovat saatavilla vain niiden käyttöön oikeutetuilla. Eheys tarkoittaa, että tietoja eivät voi muuttaa muut kuin siihen oikeutetut, kun taas käytettävyyden tarkoitus on taata, että tiedot ja tietojärjestelmät ovat niiden käyttöön oikeutettujen hyödynnettävissä (Kyberturvallisuuskeskus, 2023).

Perinteisenä CIA-kolmiona tunnettu kokonaisuus viittaa tietojärjestelmien tietoturvan peruselementteihin. Nämä kolme termiä ovat muovanneet ja laajentaneet teoreettista käsitystä tietoturvasta, sekä muokanneet käytäntöjä, joiden avulla tietoturvaa kehitetään ja toteutetaan organisaatioissa. (Samonas & Coss, 2014). Tutkimuksessa (Samonas & Coss, 2014) kerrotaan myös, että CIA-kolmiota on arvosteltu sen kapeakatseisuudesta tietotekniseen puoleen, ja myös sen rajallisesta käyttökelpoisuudesta, kun otetaan huomioon organisaation turvallisuuden hallinnolliset ja sosiaaliset näkökulmat. Tietoturvan ammattilaiset arvostavat kuitenkin edelleen CIA-kolmion antamia elementtejä, koska se tarjoaa suoraviivaisen tavan ymmärtää ja käsitellä tietoturvaan liittyviä ongelmia. Myöskään tiedeyhteisö ei ole hylännyt kolmiota, mutta siihen pyritään tekemään parannuksia, lisäämällä siihen keskeisiä termejä laajentamaan kolmijakoa. Laajentamisen tarkoituksena on lisätä kolmion soveltamisalaa vastaamaan paremmin nykypäivän vaatimuksia.

3.2 Tietoturvan ylläpitäminen ja tavoitteet

CIA-kolmion juuret ovat lähtöisin sotilaallisesta turvallisuusajattelusta, jossa on aina pyritty suojelemaan tietoja ulkoisilta uhkilta. Nykypäivän tietoturva-ammattilaisten ja akateemisten tutkijoiden lähestymistavat ovat kehittyneet tästä sotilaallisesta turvallisuusnäkemyksestä, painottaen hieman eri näkökulmia (Samonas & Coss, 2014).

Tietoturvan tavoitteena on varmistaa liiketoiminnan jatkuvuus, taloudellisten vahinkojen ehkäisy, sekä tietoturvaongelmien vaikutusten minimoiminen (Von Solms, 1998). Tietoturvan tarkoitus ja tavoite muuttuu ajan mukana. Kymmenen vuotta Von Solmsin tutkimuksen (1998) jälkeen Ashenden kuvailee tutkimuksessaan (2008) tietoturvaa seuraavasti: ”Tietoturva-ala on laajentunut viime vuosina – tekninen käsite, joka on nimetty tietoturvaksi, on laajentunut enemmän liiketoimintaan keskittyneeksi välineeksi, joka pyrkii suojelemaan informaation kaikkia muotoja, koko organisaatiossa. Tavoitteena ei ole enää pelkästään suojella CIA-kolmion osia, vaan tietoturvan avulla yritetään tuottaa todellisia liiketoimintahyötyjä, sekä suojaamalla tietoa, että helpottamalla tietojen hallittua jakamista, ja niihin liittyvien riskien hallintaa muuttuvassa uhkaympäristössä.

4 Tekoäly tietoturvan kehittäjänä

Tässä luvussa pyritään vastaamaan tutkielman esittämään tutkimuskysymykseen. Luku koostuu kahdesta alaluvusta. Ensimmäisessä alaluvussa käydään läpi keinoja, joilla tekoälyä hyödynnetään nykypäivänä yrityksissä. Toisessa alaluvussa tarkastellaan haasteita, joita tekoälyn hyödyntäminen nykypäivänä tuo mukanaan.

4.1 Tekoälyn vahvuudet yrityksen tietoturvan kehittämisessä

Digitalisaation ja verkkoteknologioiden kehittyessä, yrityksien tietoturva on yhä suurempien haasteiden edessä. Perinteiset tietoturvan taanneet teknologiat eivät enää riitä jatkuvasti kasvaville yrityksille, jolloin heidän on pakko hyödyntää uusia teknisiä keinoja tietoturvan takaamiseksi ja riskien hallitsemiseksi. Monet yritykset ovat alkaneet hyödyntää massadataa ja tekoälyä riskienhallinnassaan (Wang ym., 2023). Yksi tekoälyn suurimmista vahvuuksista onkin se, että tekoäly päivittää itsensä automaattisesti, ja kehittyy elinkaarensa kautta (Dhingra ym., 2016).

Teknologia	**Vahvuudet**	**Lähde**
Tekoäly, yleinen	Mukautumiskyky, kehittyy elinkaarensa kautta	Dhingra ym., 2016; Ailisto ym., 2018; Kaplan & Haenlein, 2019
	Suurien tietomäärien nopea käsittely ja analysoiminen	Mughal, 2018; Kaul ym., 2020
	Toiminnanohjaus ja päätöksenteon avustaminen	Dhingra ym. 2016
	Riskienhallinta (tunnistus ja suunnittelu)	Wang ym., 2023
	Tekoälyavusteinen turvallisuuskoulutus	Dash & Anisari, 2022
Tekoäly, syväoppiminen	Tunkeutujien havaitsemis- ja estojärjestelmä	Rehman & Saba, 2014; Gupta ym., 2022
	Haittaohjelmien luokittelu	Gupta ym., 2022

TAULUKKO 1 Tekoälyn vahvuudet yrityksen tietoturvan kehittämisessä

Mughalin (2018) hieman vanhan, mutta nykypäivääkin hyvin kuvaavan tutkimuksen mukaan tekoälyn vahvuudet nousevat nykypäivänä enemmän esille hyökkäysten muuttuessa monimutkaisemmiksi ja kehittyneimmiksi. Perinteiset sääntöihin pohjautuvat turvajärjestelmät eivät riitä nykypäivän uhkien torjuntaan. Tekoäly tarjoaa edistyneen ja mukautuvan lähestymistavan tietoturvaan. Yksi tekoälyn suurimmista vahvuuksia onkin suurien tietomäärien nopea käsittely ja analysoiminen, jonka ansiosta tekoälyalgoritmit voivat havaita datasta poikkeamia ja epätavallista toimintaa, mikä voi olla merkki tietoturvaloukkauksesta. Tekoälyn avulla on myös mahdollista automatisoida toimenpiteitä tietoturvaongelmien sattuessa.

4.2 Tekoälyn hyödyntäminen tietoturvan tukena

Tietoturvan tärkein tavoite on organisaation tärkeimpien resurssien, kuten laitteistojen, ohjelmistojen ja taloudellisten resurssien turvaaminen. Oikeiden tietoturvamenetelmien valinnalla organisaatio kykenee saavuttamaan tavoitteensa tietoturvan osalta. Tekoälyteknologiat toimivat erittäin hyvin toiminnanohjaustilanteissa, minkä lisäksi ne pystyvät tukemaan ihmisiä myös johtamisessa ja päätösten teossa (Dhingra ym., 2016).

Dash ja Ansari kertovat vuonna 2022 julkaistussa tutkimuksessaan, että tekoälyä käytetään nykypäivänä hyökkäyksiltä puolustautumiseen, sekä hyökkäämiseen. Tutkimuksessa (2022) myös kehutaan tekoälyn olevan siunaus moderneilta tietoturvaongelmilta suojautuessa. Dash ja Ansari jakavat tekoälyn käytön tiedon turvaamisessa seuraavasti: (1) tekoälyä käytetään tietoturvaongelmien ilmetessä, tai (2) tekoälyä käytetään aktiivisesti tietoturvaongelmien ehkäisyyn ja torjuntaan. Ensimmäinen tapa toimii organisaatioille, jotka haluavat oppia tekoälyn hyödyntämisen ja tietoturva-alan kokonaisvaltaisesti. Toinen tapa on paremmin hyödynnettävissä organisaatioille, joilla on käytössään kokeneita tietoturvan ammattilaisia, jotka pyrkivät torjumaan kaikki tietoturvaan kohdistuvat uhat. Myös tekoälyä hyödyntävän käyttäytymiseen perustuvan turvallisuuskoulutuksen käyttö on heidän mukaansa lisääntymässä startup-yrityksissä ja huipputekniikan yrityksissä, jotka ovat kasvattamassa suosiotaan nuoren yleisön keskuudessa. Kaikkien uhkien torjuntaan pyrkivä järjestelmä on vaikea toteuttaa.

Rehmanin ja Saban vuonna 2014 julkaistussa tutkimuksessa kerrotaan, että lujatekoisten tunkeutumisen havaitsemis- ja estojärjestelmien suunnittelu ja kehittäminen on riippuvainen kolmen keskeisen alueen tiedoista, luokitus- ja mallintamistekniikoista ja järjestelmän infrastruktuurista. Jokaisella osa-alueella on omat erityispiirteensä, -tekniikkansa ja -rajoituksensa, mutta yhdessä ne voivat edistää sellaisen järjestelmän kehittämistä, jolla varmistetaan: (1) epävarmuuden vähentäminen käyttäjien käyttäytymisen profiloinnissa, (2) herkkyyden ja tarkkuuden lisääminen (3) reaaliaikainen reagoiminen uhkiin. (Rehman & Saba, 2014.)

Syväoppiminen, joka on yksi merkittävimmistä tekoälyn osa-alueista, on edistynyt merkittävästi tietoturvaongelmien ratkaisemisessa. Teknologian avulla voidaan luoda monimutkaisia malleja tunkeutumisen havaitsemiseksi, luokitella haittaohjelmia sekä havaita kyberuhkia verkossa (Gupta ym., 2022). Näyttääkin siltä, että syväoppimisen avulla kehitetyt järjestelmät ovat ratkaisu Rehmanin ja Saban (2014) pohtimalle lujatekoiselle tunkeutumisen havaitsemis- ja estojärjestelmälle.

5 Yhteenveto ja pohdinta

Tämän tutkielman tarkoituksena oli tarkastella tekoälyä, tietoturvaa sekä tapoja joilla tekoälyä voidaan hyödyntää tietoturvan kehittämisessä. Tutkielman tavoitteena oli löytää tapoja, joilla tietoturvaa voidaan kehittää tekoälyn avustuksella. Tutkielman tutkimuskysymys on seuraava :

- Miten tekoälyä voi hyödyntää yrityksen tietoturvan kehittämiseen?

Tutkielman neljännessä luvussa käytiin läpi tekoälyn käyttömahdollisuuksia tietoturvan kehittämisessä. Tutkielmassa havaittiin, että tekoälyllä on monia hyödyllisiä ominaisuuksia, joita hyödyntämällä yrityksien tietoturvaa on mahdollista kehittää. Tekoälyn vahvuudet korostuvat suurien tietomäärien käsittelyssä ja analysoimisessa, mikä tekee siitä tehokkaan työkalun yrityksen tietoturvan ylläpitämisessä sekä kehityksessä. Tekoäly myös mukautuu uusiin tilanteisiin automaattisesti, ja kehittää omaa toimintaansa kokemuksien avulla, mikä tekee tekoälystä tehokkaan työkalun yrityksen tietojen turvaamisessa.

Tutkielman ensimmäisessä sisältöluvussa määriteltiin tekoäly, kerrottiin sen historiasta sekä tutkittiin tekoälyn eri muotoja. Luvun perusteella voidaan päätellä, että tekoälyn määrittely on haastavaa ja vaihtelevaa, mutta määritelmistä löytyy yhteisiä piirteitä, kuten mukautumiskyky ja oppimiskyky. Tekoälyn synnylle ei ole tiedossa tarkkaa ajankohtaa, mutta sen voidaan katsoa alkaneen kehittyä kunnolla 1950-luvulla, kun ensimmäiset älykkyyttä jäljittelevät ohjelmat julkaistiin ja tekoälyn käsite syntyi. Kehitysvauhti nykypäivään on ollut vaihtelevaa. Teknologia on kehittynyt harppauksina aiheeseen liittyvien teknologioiden mukana. Nykypäivänä aihetta tutkitaan aktiivisesti, minkä vuoksi kehitystä on tapahtunut huomattavasti nopeammin kuin aikaisempina vuosikymmeninä.

Toisessa sisältöluvussa käsiteltiin tietoturvan perusteita hyvin pelkistetyllä tasolla, aiheen laajuuden vuoksi. Luvussa opittiin tietoturvan klassinen CIA-kolmio, joka on paljon käytetty ja myös kritisoitu perusta tietoturvan ylläpitämiselle organisaatioissa. Luvussa kerrottiin myös tietoturvan tavoitteet: yrityksen liiketoiminnan jatkuvuuden turvaaminen, tietoturvaongelmien vaikutuksien minimoiminen ja taloudellisten vahinkojen ehkäisy.

Tutkielman kolmannessa sisältöluvussa käsiteltiin tekoälyn mahdollisuuksia tietoturvan kehittäjänä ja pyrittiin esittelemään tekoälyn käytön mahdollisuuksia tietoturva-alalla sekä eri tekoälyteknologioiden vahvuuksia. Tekoälyteknologioista suurimmassa roolissa on syväoppiminen, joka kykenee luomaan monimutkaisia malleja hyökkäysten havaitsemiseen sekä torjuntaan, minkä lisäksi se kykenee haittaohjelmien luokitteluun.

Maailman muuttuessa yhä enemmän digitaaliseksi yrityksien on muututtava sen mukana. Digitalisaation vuoksi yritysten tietoturvaan kohdistuu yhä enemmän uhkia, tietojen löytyessä verkosta eikä paperiversiona. Digitalisaatio nostaa tietoturvan merkityksen entistä korkeammalle, mikä luo tarpeen uusille toimintatavoille ja ratkaisuille. Ihminen toimii harvoin täysin rationaalisesti, minkä

vuoksi tekemämme päätökset eivät ole aina optimaalisia. Tekoälyjärjestelmän hyödyntäminen päätöksien apuna nostaa ihmisen suorituskykyä, jolloin parempiin päätöksiin on helpompi päästä. Tässä tutkielmassa nostettiin esiin keinoja, joiden avulla tekoälyteknologioita voidaan hyödyntää tehokkaamman tietoturvan rakentamisessa yrityksille. Aiheesta on löydettävissä suhteellisen vähän tutkimustietoa, minkä vuoksi tarve jatkotutkimukselle on suuri. Lisäksi jatkotutkimusta voisi tehdä käsittelemällä tarkemmin aiheeseen liittyviä käsitteitä ja teknologioita.

LÄHTEET

Ailisto, H., Neuvonen, A., & Seppälä, T. (2018). Tekoälyn kokonaiskuva ja osaamiskartoitus.

Ashenden, D. (2008). Information Security management: A human challenge? *Information Security Technical Report*, 13(4), 195–201. https://doi.org/10.1016/j.istr.2008.10.006

Choi, R. Y., Coyner, A. S., Kalpathy-Cramer, J., Chiang, M. F., & Campbell, J. P. (2020). Introduction to Machine Learning, Neural Networks, and Deep Learning. *Translational Vision Science & Technology*, 9(2), 14. https://doi.org/10.1167/tvst.9.2.14

Dash, B., & Ansari, M. F. (2022). An Effective Cybersecurity Awareness Training Model: First Defense of an Organizational Security Strategy. 9, 2395–0056.

Davenport, T., & Kalakota, R. (2019). The potential for artificial intelligence in healthcare. *Future Healthc* J, 6(2), 94–98. https://doi.org/10.7861/futurehosp.6-2-94

Dhingra, M., Jain, M., & Jadon, R. S. (2016). Role of artificial intelligence in enterprise information security: A review. *2016 fourth international conference on parallel, distributed and grid computing (PDGC)*, 188–191.

Gupta, C., Johri, I., Srinivasan, K., Hu, Y.-C., Qaisar, S. M., & Huang, K.-Y. (2022). A Systematic Review on Machine Learning and Deep Learning Models for Electronic Information Security in Mobile Networks. *Sensors*, 22(5), Article 5. https://doi.org/10.3390/s22052017

Haenlein, M., & Kaplan, A. (2019). A Brief History of Artificial Intelligence: On the Past, Present, and Future of Artificial Intelligence. *California Management Review*, 61(4), 5–14. https://doi.org/10.1177/0008125619864925

Hu, Y., Kuang, W., Qin, Z., Li, K., Zhang, J., Gao, Y., Li, W., & Li, K. (2021). Artificial Intelligence Security: Threats and Countermeasures. *ACM Computing Surveys*, 55(1), 20:1-20:36. https://doi.org/10.1145/3487890

Kaplan, A., & Haenlein, M. (2019). Siri, Siri, in my hand: Who's the fairest in the land? On the interpretations, illustrations, and implications of artificial intelligence. *Business Horizons*, 62(1), 15–25. https://doi.org/10.1016/j.bushor.2018.08.004

Kaul, V., Enslin, S., & Gross, S. A. (2020). History of artificial intelligence in medicine. *Gastrointestinal Endoscopy*, 92(4), 807–812. https://doi.org/10.1016/j.gie.2020.06.040

Kyberturvallisuuskeskus. (2023). https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/saantely-ja-valvonta/tietoturva

LeCun, Y., Bengio, Y., & Hinton, G. (2015). Deep learning. *Nature*, 521(7553), Article 7553. https://doi.org/10.1038/nature14539

Mughal, A. A. (2018). Artificial Intelligence in Information Security: Exploring the Advantages, Challenges, and Future Directions. *Journal of Artificial Intelligence and Machine Learning in Management*, 2(1), Article 1.

Rehman, A., & Saba, T. (2014). Evaluation of artificial intelligent techniques to secure information in enterprises. *Artificial Intelligence Review*, 42(4), 1029–1044. https://doi.org/10.1007/s10462-012-9372-9

Russell, S. J. & Norvig, P. (2016). Artificial Intelligence: A Modern Approach. 3. painos. *Harlow: Pearson Education Limited*.

Samonas, S., & Coss, D. (2014). The CIA Strikes Back: Redefining Confidentiality, Integrity and Availability in Security. *Journal of Information Systems Security*, 10(3), 21-45

Sayler, K. M. (2020). Artificial Intelligence and National Security. *Congressional Research Service.*

Shinde, P. P., & Shah, S. (2018). A Review of Machine Learning and Deep Learning Applications. *2018 Fourth International Conference on Computing Communication Control and Automation (ICCUBEA*), 1–6. https://doi.org/10.1109/ICCUBEA.2018.8697857

Smith, K. A., & Gupta, J. N. D. (2000). Neural networks in business: Techniques and applications for the operations researcher. *Computers & Operations Research*, 27(11–12), 1023–1044. https://doi.org/10.1016/S0305-0548(99)00141-0

Vartiainen, H., Tedre, M., Jormanainen, I., Kahila, J., & Valtonen, T. (2021). Tekoäly, koneoppiminen ja teknologinen murros: Kohti datatoimijuutta ja tulevaisuuden design-taitoja. https://erepo.uef.fi/handle/123456789/26807

Von, S. R. (1998). Information security management (3): The Code of Practice for Information Security Management (BS 7799*). Information Management & Computer Security*, 6(5), 224–225. https://doi.org/10.1108/09685229810240158

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

Wang, Q., Zong, B., Lin, Y., Li, Z., & Luo, X. (2023). The Application of Big Data and Artificial Intelligence Technology in Enterprise Information Security Management and Risk Assessment. *Journal of Organizational and End User Computing(JOEUC)*,35(1), 1–15. https://doi.org/10.4018/JOEUC.326934

Wilson, H. J., Daugherty, P. R., & Morini-Bianzino, N. (2018). The Jobs That Artificial Intelligence Will Create. *Mit Sloan Management Review, What the Digital Future Holds* (ss. 97–104). The MIT Press. https://doi.org/10.7551/mitpress/11645.003.0020