Oskari Suvilehto

TEKOÄLYN HYÖDYNTÄMINEN HAJAUTETTUJEN PALVELUESTOHYÖKKÄYSTEN HAVAITSEMISESSA

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2024

TIIVISTELMÄ

Suvilehto, Oskari
Tekoälyn hyödyntäminen hajautettujen palveluestohyökkäysten havaitsemisessa
Jyväskylä: Jyväskylän yliopisto, 2024, 21 s.
Tietojärjestelmätiede, kandidaatintutkielma
Ohjaaja: Clements, Kati

Hajautetut palveluestohyökkäykset eli DDoS-hyökkäykset pystyvät aiheuttamaan merkittäviä vahinkoja, kun palvelujen tai laitteiden toimintakyky estetään ruuhkauttamalla verkkoliikenne. Ongelmana tässä on, että perinteiset DDoS havaitsemismenetelmät eivät riitä enää uusiin mukautuviin hyökkäyksiin. Tämän tutkielman tarkoituksena oli löytää käyttäen tämän päivän kehittynyttä tekoälyä mahdollisiin ratkaisuihin havaita DDoS-hyökkäyksiä. Tutkielma oli toteutettu kirjallisuuskatsauksena, jossa hyödynnetty alan tieteellisiä artikkeleita ja kirjallisuutta. Kirjallisuuskatsauksessa ratkaisuna tutkimusongelmaan löytyi erilaisia tekoälymenetelmiä, joita pystytään käyttämään DDoS-hyökkäysten havaitsemiseen. Osa käsitellyistä menetelmistä pystyi hyvin tarkkoihin tuloksiin. Tärkeää on kumminkin huomioida oikeanlaisen menetelmän valikointi, jotta voidaan päästä tarpeeksi tarkkaan tulokseen DDoS-hyökkäysten havaitsemiseen. Tutkimus korosti, että tekoälymenetelmien onnistunut toiminta edellyttää riittävän ajantasaisen opetusdatan hyödyntämistä, jotta nämä menetelmät voivat torjua myös uusia ja kehittyneempiä DDoS-hyökkäyksiä.

Asiasanat: Algoritmit, DDoS, Hajautettu palvelunestohyökkäys, Kyberturvallisuus, Tekoäly.

ABSTRACT

Suvilehto, Oskari
Utilizing Artificial Intelligence in Detecting Distributed Denial of Service Attacks
Jyväskylä: University of Jyväskylä, 2024, 21 p.
Information systems science, bachelor's thesis
Supervisor(s): Clements, Kati

Distributed Denial of Service attacks, or DDoS attacks, can cause significant damage by disrupting the functionality of services or devices through network traffic congestion. The problem lies in the fact that traditional DDoS detection methods are no longer sufficient to counter new, adaptive attacks. The purpose of this thesis was to explore potential solutions for detecting DDoS attacks using today's advanced artificial intelligence. The study was conducted as a literature review, utilizing scientific articles and literature from the field. In the literature review, various artificial intelligence methods were found as a solution to the research problem, which can be used to detect DDoS attacks. As solutions, various artificial intelligence methods can be used to detect DDoS attacks. Some of the methods reviewed demonstrated very high levels of accuracy. However, it is important to consider selecting method in order to achieve a sufficiently accurate result for detecting DDoS attacks. The study highlighted that the successful performance of AI methods relies on utilizing sufficiently up-to-date training data to ensure these methods can also counter new and more advanced DDoS attacks.

Keywords: Algorithms, DDoS, Distributed denial-of-service attack, Cybersecurity, Artificial intelligence.

TAULUKOT

SISÄLLYS

1 Johdanto

Teknologia kehittyy ja niin kehittyy myös siihen kohdistuvat uhat, jotka pyrkivät estämään teknologian käytettävyyttä. Brooks ym. (2021) selittivät, miten hajautetulla palveluestohyökkäyksillä eli DDoS-hyökkäyksillä pystytään merkittävästi tuhoamaan halutun laitteen käytettävyys ylikuormittamalla sen resurssit, kuten palvelimen kapasiteetin tai kaistaleveyden pyynnöillä. Osterweil ym. (2020) totesivat, mitä tulee DDoS-hyökkäyksiin, että ovat nekin kehittyneet kahdessakymmenessä vuodessa hyökkäykseen käännytettyjen bottien määränä sadoista tai tuhansista miljooniin. Internettiin myös tallennetaan yhä enemmän arkaluontoista ja tärkeää materiaalia, jonka vuoksi tavoittelevat tahot pyrkivät hyökätä yhä enemmän ja aiheuttaa vahinkoa yhteisöille mm. taloudellisilla tai terveydellisillä vahingoilla (Awan ym., 2021).

Näitä DDoS-hyökkäyksiä varten on hyvä löytää sopivia havaitsemismenetelmiä, joita Kaur ym. (2017) käsittelivät artikkelissaan. Kaur ym. (2017) totesivat tekstissään ongelman, sillä monet perinteiset menetelmät eivät olisi riittävän tehokkaita tällaiseen reaaliaikaiseen havaitsemiseen. Lisäksi ongelmana on, etteivät ne saavuta korkeaa tarkkuutta ja antavat vääriä hälytyksiä. Khalef ym. (2019) ovat myös todenneet ongelman DDoS-hyökkäysten havaitsemisessa vanhempien turvajärjestelmä tekniikoiden kanssa. Khalef ym. (2019) näkevät taas paljon hyvää tekoälypohjaisessa havaitsemistekniikassa, jolla voitaisiin tarjota mahdollisuutta joustavuuteen ja kykyyn mukautua reaaliaikaisesti hyökkäyksiin.

Tekoäly kumminkin nykypäivänä varsin kehittynyttä ja määritelty Russellin ja Norvigin (2010) mukaan, että tekoäly toimii järjestelmänä, joka pystyy vastaanottaa havaintoja ympäristöstään ja suorittaa siihen perustuvia toimintoja. Alghoson ja Abbass (2021) kertoivat tarkemmin artikkelissaan tekoälyn ja tarkemmin ottaen koneoppimisen eri mallien tutkimisesta DDoS-hyökkäysten havaitsemisessa sekä niiden merkittävästä tehokkuudesta ja tarkkuudesta mihin koneoppimisella pystytään. Ratkaisuja on siis löydettävissä DDoS-hyökkäysten havaitsemiseen nykyteknologialla Alghoson ja Abbassin (2021) mukaan.

Tässä tutkielmassa käydään läpi tärkeinä teemoina näitä tekoälyteknologioita ja palvelunestohyökkäyksiä. Näiden aiheiden käsittelyn jälkeen

siirrytäänkin aiheeseen, jossa käydään läpi, miten voitaisiin löytää ratkaisuja tähän DDoS-hyökkäysten havaitsemisen ongelmaan hyödyntäen tekoälyteknologioita. Tutkimuskysymys on muotoiltu seuraavasti:

- Miten tekoälyä voitaisiin hyödyntää hajautettujen palveluestohyökkäysten havaitsemisessa?

Kyseistä aihetta on tärkeää tutkia, koska se voi aiheuttaa merkittäviä taloudellisia ja toiminnallisia vahinkoja organisaatioille tai yksityishenkilöille. Motivaationa tälle kyseiselle tutkimukselle toimii se, miten tekoälyteknologioita voidaan hyödyntää tavalla, joka tukee kyberhyökkäysten ennakoivaa havaitsemista sekä siten myös niiden ehkäisyä. Kyberhyökkäykset ja niiden torjunta on ajankohtainen ja merkittävä aihe niiden lisääntyessä ja tämän vuoksi on tärkeää pohtia ratkaisujaongelmaan.

Tämän tutkielma toteutusmuoto on kirjallisuuskatsaus. Kirjallisuuskatsauksessa hyödynnettyä aineistoa on haettu seuraavista tieteellisten julkaisuiden hakukoneista, kuten JYUDOK, Google Scholar, IEEE Xplore ja Springer. Hakusanoina on käytetty keskeisiä termejä tutkimukselle kuten esim. “DDoS”, “Artificial Intelligence”, “distributed denial of service detection”. Näitä hakusanoja myös yhdisteltiin aineiston haussa.

Tutkielma etenee seuraavalla tavalla. Ensin lähdetään käsittelemään määritelmää tekoälynmääritelmää, kehityskaarta ja tämän myötä tekoälyn vahvuuksia ja heikkouksia, jonka jälkeen mietitään, miten tekoälyä voidaan soveltaa kyberturvallisuuteen. Tästä siirrytään DDoS-hyökkäysten määritelmään, erilaisiin hyökkäystyyppeihin ja näiden vaikutuksiin, joka johtaa perinteisiin DDoS-hyökkäysten havaitsemismenetelmiin ja niihin liittyviin heikkouksiin. Tämä johtaa siihen, että pääsemme käsittelemään, miten tämä tekoäly toimii DDoS-hyökkäysten havaitsemisessa. Lisäksi tuodaan esille, kuinka tarkasti nämä tekoälymenetelmät pystyvät havaitsemaan näitä DDoS-hyökkäyksiä, sekä tuodaan esille tähän liittyviä mahdollisia haasteita. Yhteenvedossa on tarkoituksena käsitellä tuloksia tekoälyn menetelmien havaitsemiskyvykkyyksistä, sekä arvioida ja vertailla näiden menetelmien sopivuutta DDoS-hyökkäysten havaitsemiseen.

2 Tekoälyn perusteet ja soveltaminen kyberturvallisuudessa

Tämä luku sisältää tekoälyteknologioiden läpikäyntiä. Aluksi luvussa käydään läpi tekoälyn määritelmää ja hieman kehityskaarta läpi. Tämän jälkeen siirrytään käsittelemään tekoälymenetelmiä, jonka jälkeen käsitellään tekoälyyn kohdistuvia heikkouksia ja vahvuuksia. Viimeisenä kappaleessa käydään läpi tekoälyn mahdollisuutta kyberturvallisuudessa ja siihen liitettäviä sovelluksia.

2.1 Tekoälyn määritelmää ja kehityskaari

Tekoäly ja sen määritelmä voidaan käsittää Russell ja Norvig (2010) mukaan järjestelmänä, joka mukautuu ympäristöön havainnoiden sitä ja suorittaa siihen perustuvia toimintoja. Jiang ym. (2022) kertoivat myös näkemyksensä tekoälyn määritelmästä, että tekoäly on mahdollistamassa koneita tekemään toimintoja, jotka vaativat ihmisen älykkyyttä.

Russell ja Norvig (2010) käsittelivät tekoälyn kehityskaarta läpi omassa tuotoksessaan. Tämä tekoälyn kehitys on lähtenyt liikkeelle 1940–50 luvulla, kun Warren McCulloch ja Walter Pitts loivat keinotekoisen neuronimallin, jonka toiminta perustui aivojen neuronien fysiologiseen toimintaa ja loogiseen laskentaan. Myöhemmin Alan Turing esitti idean koneiden oppimisesta, ja vuonna 1956 tuotiin termi tekoäly esille. Tämän jälkeen kehitys hidastui 1980-luvulle asti, kunnes neuroverkot ja koneoppiminen tuotiin takaisin esille. Tästä kehitys on kasvanut 2000-luvun suurien datamassojen hyödyntämisestä ja kehittyneiden laskentamenetelmien myötä. Nyt tekoäly on kehittynyt paljon laskentatehon kasvun ja tieteellisien menetelmien yleistymisen myötä. (Russell ja Norvig, 2010.)

Tekoäly on kehittynyt niin paljon, että se voidaan nähdä nykypäivänä teknologian tukipilarina, sekä myös sen käsitteellä nähdään yhä syvällisempi vaikuttus ihmiselämään. Tekoälyä on pystytty soveltamaan laajalti eri aloille, kuten terveydenhuoltoon, teollisuuteen, kuljetukseen ja koulutukseen. Myös tekoäly itsessään nähdään merkittävänä markkinana ja yhdistetyllä vuotuisella kasvuvauhdilla ennustettu vuoteen 2025 kasvavan jopa 190 miljardiin dollariin. (Jiang ym., 2022.)

2.2 Tekoälymenetelmiä

Sarker (2021) selitti tekoälyn osa-alueesta nimeltä koneoppiminen. Koneoppiminen on määritelty julkaisussa keinona, jolla voitaisiin järjestelmille saada kyvyn oppia, sekä myös parantaa omaa suorituskykyään kokemuksen myötä. (Saker, 2021).

Saker (2021) luokitteli koneoppimisen eri algoritmit 4 eri pääkategoriaan. Ensimmäisenä valvottu oppiminen, joka on oppimismenetelmä, jossa algoritmi esimerkin avuin pystyy oppimaan syötedatasta ja oikeista vastauksista eli

tulosluokista toimintatavan. Toinen oppimismenetelmä on valvomaton oppiminen, jossa ei ole valmiita luokkia tai ennustettavia arvoja vaan se luo ne itse datasta havaitsemalla merkityksellisiä piirteitä. Seuraava menetelmä on puolivalvottu oppiminen, jossa yhdistetään kaksi aikaisempaa menetelmää. Se pyrkii hyödyntämään merkittyä ja merkitsemätöntä dataa, kun merkittyä on vähän ja merkitsemätöntä dataa on paljon. Viimeinen oppimismalli on vahvistusoppi ja se perustuu palkitsemiseen ja rankaisemiseen eli tämä toimii palautteen perusteelta. Tässä siis algoritmi saa palautetta ympäristöltään ja pyrkii tämän myötä parantaa tehokkuutta. (Saker, 2021.)

LeCun ym. (2015) kertoivat vähän erilaisemmasta koneoppimisen teknologiasta, joka kuuluu neuroverkkojen ja edustuksenoppimiseen nimeltä syväoppiminen. Tämä menetelmä perustuu monikerroksisiin hermoverkkoihin, joka lähtee liikkeelle syötetyn datan yksinkertaisista piirteistä ja havaitsee aina korkeammilla kerroksilla yhä abstraktimpia ja monimutkaisempia asioita syötteestä. Tämä algoritmin toiminta tapahtuu ilman ihmisen suunnittelemia piirteitä. (LeCun ym., 2015.)

On olemassa myös tekoälymenetelmä, joka nimeltään dendriittisolualgoritmi eli DCA. Tämä algoritmi perustuu ihmisellä olevaan immuunijärjestelmään ja lisäksi erityisesti vaarateoriaan. Tämä järjestelmä toimiin niin, että se pystyy havaitsemaan ja reagoimaan vaaratilanteisiin eli havaitsee vaarasignaaleja ja turvallisia signaaleja, jota ohjaavat ja havaitsevat soluagentit. (Igbe ym., 2017.)

2.3 Tekoälyn vahvuudet ja haasteet

Tekoälyn erityisenä vahvuutena voi nähdä sen rationaalisuus. Tekoäly tekee päätöksiä sille syötetyn tiedon perusteella, mikä on merkittävää, kun tarvitaan nopeita ja tarkkoja päätöksiä ilman ylimääräisiä pohdintoja. Myös tekoälyn kyvykkyys mukautua erilaisiin uusiin olosuhteisiin ja kyky toimia niissä voidaan nähdä vahvuutena. (Russell ja Norvig, 2010.) Tekoälyn kyvykkyys oppia itse on myös vahvuus, sillä se pystyy luomaa omia, strategiota itse kuten AlphaGo Zero-järjestelmä on tekoälyn luoma (Jiang ym., 2021). Kaur ym. (2017) myös kertoivat tekoälyn vahvuudesta, että se kykenee havaitsemaan poikkeavuuksia ja kaavoja suurista datamassoista. Tekoälyn avulla voidaan myös vähentää kuluja muun muassa, kun otetaan käyttöön tekoäly verkko välitteisessä asiakaspalvelussa tai se vähentää ihmisten tuottamia virheiden kustannuksia. Tekoälyn avulla voidaan myös parantaa resurssien optimointia, kun se analysoi suuria määriä dataa, mikä on yhdistetty IoT-laitteisiin. Tekoäly pystyy myös parantamaan tuotantoprosesseja, kun se analysoi teollisuudessa käytettyjen robotiikka- ja konenäköjärjestelmien tuottamaa dataa. (Dinmohammadi 2023.)

Haasteitakin voi tulla tekoälyllä vastaan, kuten esim. tekoälyn käyttäminen voi vaatia suurta laskentatehoa. Tekoälyn käyttöönotto voi olla myös aikaa vievää, nimittäin oppisprosessi voi vaatia suuria määriä dataa analysoitavaksi. (Kaur ym., 2017.) Tekoälyn suoriutumiskyvyssäkin voi tulla haasteita vastaan, mikäli datan laatu on heikkoa ja määrällisesti liian vähäistä. Tämä voi johtaa tilanteisiin, missä järjestelmä ei osaa tulkita tilanteita oikein. (Russell ja Norvig,

2010.) Yhtenä keskeisenä haasteena nähdään myös IT-infrastruktuuri, resurssit ja tekoäly osaajien puute, joka vaikuttaa tekoälyn käyttöönottoon (Dinmohammadi, 2023).

2.4 Tekoälyn sovellukset kyberturvallisuudessa

Suthishni ja Kumar (2022) kertoivat, miten monipuolisesti tekoälyä voidaan soveltaa kyberturvallisuudessa. Tässä käsitellään miten tunkeutumis- havaitsemisjärjestelmiin (IDS) voitaisiin sisällyttää koneoppimismenetelmiä. Nämä koneoppimismallit ovat sijoitettu anomaliapohjaiseen malliin, sillä se osaa havaita hyvin järjestelmälle tulevia tuntemattomia uhkia. Nämä koneoppimismallit ovat taas jaettu perinteisiin koneoppimismalleihin ja syväoppimismalleihin. IDS-järjestelmiin sopivat perinteiset koneoppimismallit, on jaettu valvottuihin, valvomattomiin ja yhdistemalleihin. IDS:ään sopivat syväoppimallit luokiteltiin valvottuihin ja valvomattomiin syväoppimismalleihin. (Suthishni ja Kumar, 2022.)

Folowo ym. (2023) korostivat julkaisussaan tekoälyn merkittävyyttä verkkoliiketeen seurannassa. Tämä korostaa, että tekoälyä ja tarkemmin ottaen koneoppimista tulisi hyödyntää DDoS-hyökkäysten havaitsemisessa kyberturvallisuuden parantamiseksi. Verkkoliiketeessä tapahtuva liikenteen määrä on niin valtava, että se on liian suuri ihmisen analysoitavaksi ja tämän vuoksi tulisi käyttää koneoppimiseen perustuvaa järjestelmää verkkoliikenteen seurannassa. (Folowo ym., 2023.)

Asad ym. (2020) kertoivat julkaisussaan syväoppimisen mahdollisuuksista DDoS-hyökkäysten havaitsemisessa. Syvät neuroverkot pystyvät käymään läpi pakettivirtojen merkittäviä ominaisuuksia monikerroksisen rakenteen vuoksi, jonka avulla se pystyy havaitsemaan vaikeasti havaittavia hyökkäyksiä (Asad ym., 2020).

SDN-verkkojen eli ohjelmallisesti määritelty verkot ovat erityisen alttiita DDoS-hyökkäyksille keskitetyn hallintarakenteensa vuoksi. Tämän vuoksi näihin on hyvä käyttää hybridi syväoppimismenetelmiä tekoäly sovelluksena, jotka ovat kolme algoritmia 1D-konvoluutioverkko (CNN), gated recurrent unit (GRU) ja dense neural network (DNN). Tämä useiden algoritmien yhdistelmä pystyy monipuolisesti havaita suuri- ja pienivolyymisiä hyökkäyksiä. (Elubeyd ja Yiltas-Kaplan 2023.)

Abu Bakar ym. (2023) julkaisussaan käsittelivät älykästä agenttipohjaista DDoS-hyökkäyksien havaitsemisjärjestelmää, joka toimii tekoäly sovelluksena kyberturvallisuuden alueella. Tässä kyseisessä menetelmässä käytetään eri tekoälymenetelmiä, sekä erityisesti syväoppimista ja koneoppimista. Näiden avulla pystytään havaitsemaan DDoS-hyökkäyksiä automaattisesti verkkoliikenteestä. Tämä kyseinen järjestelmä pitää kouluttaa, jotta se oppii havaitsemaan erot normaalin ja poikkeavan liikenteen välillä. (Abu Bakar ym., 2023.)

3 Hajautetut palvelunestohyökkäykset

Tässä luvussa käydään läpi hajautettuja palvelunestohyökkäyksiä. Kappaleessa edetään seuraavasti, hajautettuja palveluestohyökkäyksistä käydään läpi niiden määritelmää ja erilaisia hyökkäys tyyppejä. Tämän jälkeen käsitellään, mitä hajautetut palveluestohyökkäykset pystyvä aiheuttamaan. Viimeisenä aiheena käsitellään perinteisempiä havaitsemismenetelmiä, sekä niihin sisältyviä haasteita.

3.1 Hajautetun palvelunestohyökkäysten määritelmä ja tyyppejä

Hajautettu palveluestohyökkäys toisin sanoen DDoS-hyökkäysten tarkoituksena on estää jonkinlaisen palvelun tai laiteen toimintaa. Tämä hyökkäys tapahtuu käyttäen useita tietokoneita yhtäaikaisesti, jotka hyökkääjä on ottanut hallintaa eli bottiverkkoa. Tätä bottiverkkoa käyttäen pystytään ruuhkauttamaan verkkoliikenne liian suureksi. (Brooks ym. 2021.) Osterweilin ym. (2020) mukaan DDoS-hyökkäykset lähtivät liikkeelle Trin00 nimisestä haittaohjelmasta, joka kaappasi useat tietokoneet ruuhkauttamaan ja kaatamaan Minnesodan yliopiston tietoverkon. Tuosta pisteestä DDoS-hyökkäykset ovat kehittyneet satojen laitteiden bottiverkosta, jopa miljoonien laitteiden hyökkäyksiin. (Osterweil ym. 2020.)

Gupta ja Badve (2017) kertoivat tekstissään volumetrisista DDoS-hyökäyksistä. Tällaisessa hyökkäys tyypissä hyökkääjä pyrkii ottamaan haltuun koko kohteen verkkokaistan lähettämällä määrällisesti paljon paketteja kohteena olevalle palvelimelle. Tämä estää sitten normaalin verkkoliikenteen käyttäjiä käyttämästä palvelua. Esimerkkinä tähän hyökkäystyyliin toimivat UDP tai SYN tulvat. (Gupta ja Badve, 2017.)

On myös olemassa protokollapohjaisia hyökkäyksiä, jossa keskitytään volyymin sijaan verkkoprotokollien heikkouksien kuormittamista, kuten TCP SYN-hukutus. Tässä hyökkäys mallissa hyödynnetään kolmen osapuolen kättelyn rajoituksia, kun muodostetaan yhteyttä eli hyökkääjä lähettää paljon SYN-paketteja ja jättää vastaamatta palvelimen pyytämiin vastauksiin. Tämä johtaa siihen, että palvelin odottaa lopullisia ACK-paketteja asiakkaalta, jotka eivät saavu. Tilanne johtaa siihen, että palvelin ei pysty ottamaan muilta pyyntöjä vastaan, kun SYN-jono on täynnä hyökkääjän ansioista ja tämä ylittää palvelimen resurssit. (Khalaf ym., 2019.)

Kalutharage ym. (2023) kertoivat taas sovellustasoon kohdistuneista hyökkäyksistä. Tässä hyökkäys tyypissä analysoidaan haavoittuvaisuuksia ja kohdistetaan se avoimeen palvelinporttiin, joita ovat esim. HTTP-, TCP-, UDP- ja ICMP-protokollat. Hyökkääjä tekee siis tavallisen verkkoyhteyden, joka ohittaa palomuurin, jotka kautta voi aloittaa hyökkäysten. Tätä kautta hyökkääjä voi estää normaaleja käyttäjiä käyttämästä palveluja palvelimen ylirasituksen vuoksi. (Kalutharage ym., 2023.)

DDoS-hyökkäyksistä on myös erilainen tyyppi nimeltä DRDoS-hyökkäys eli reflektiohyökkäys. Tämä on kehittynyt versio DDoS-hyökkäyksestä, joka on kaksivaiheinen. Tässä DRDoS-hyökkäyksessä ensin pyritään käyttämään

hyödyksi laillisia isäntä palvelimia, jolla hyökkääjä voi huijata hyökkääjän lähdettä. Tämän vuoksi myös hyökkäysten kohteena oleva palvelu myös vastaa pyyntöihin. Näitä lähde huijattuja laitteita voidaan kutsua myös heijastimina. Toinen vaihe on käyttää näitä heijastimia hyökkäykseen, jotka ohjaavat haluttuun kohteeseen suoraan maksimi vastaukset suhteessa pyyntöön, joka ruuhkauttaa verkkoliikenteen. (Nuiaa ym., 2021.)

3.2 Hyökkäysten vaikutukset

DDoS-hyökkäykset aiheuttamat ongelmat toiminnallisuuksiin voi johtaa merkittäviin taloudellisiin tappioihin. 2007 vuonna Viro kohtasin maailman ensimmäisen itsenäistä valtiota kohtaa olleen merkittävän DDoS-hyökkäysten. Tämä aiheutti häiriöitä Viron julkinen-, pankki- ja media sektorit kokivat merkittäviä häiriöitä, kun Viron internetliikenne kasvoi 400-kertaiseksi normaalista. Häiriö aiheutti viikkojen ajan palvelujen toimintaan. DDoS-hyökkäys aiheutti Virossa taloudellisesti jopa kymmenien miljoonien tulo menetyksiä. Tämä myös aiheutti, jopa kansassa julkisen luottamuksen heikkenemisen näihin instituutioihin. (Haner ja Knake, 2021.)

Abhishta ym. (2017) kertoivat DDoS-hyökkäysten vaikutuksista, jotka voivat olla suoria tai epäsuoria taloudellisia tappioita. Suorina taloudellisina tappioina voidaan pitää verkkoliikenteen menetys, infrastruktuurin toimintakatkos, seisokit, mahdolliset lunnasrahat ja asiakaskorvaukset esimerkiksi. Epäsuoria taloudellisia tappioita voivat olla mainehaitat ja yrityksen osakekurssin lasku muuna muassa. DDoS-hyökkäykset pystyvät aiheuttaa keskeytyksiä palvelutarjontaa, joka voi johtaa jopa merkittävään osakekurssin laskuun. (Abhishta ym., 2017.)

3.3 Perinteiset havaitsemismenetelmät

Kaur ym. (2017) on kertonut perinteisemmästä DDoS-hyökkäysten havaitsemismenetelmästä nimeltä signatuuripohjainen havaitseminen. Tässä havaitsemismenetelmässä malli on opetettu havaitsemaan tunnetut hyökkäys mallit annetuista aineistoista. Tämän vuoksi se on tehokas havaitsemaan kyseisiä hyökkäyksiä. Ongelmana kumminkin on, että se ei osaa havaita uusia tai muuttuneita hyökkäysmalleja. (Kaur ym. 2017.)

Sommer ja Paxson (2010) ovat kertoneet toisesta perinteisestä havaitsemismenetelmästä, joka on nimeltään anomalia havaitseminen. Tämä on sellainen lähestymistapa, jossa järjestelmälle on luotu malli normaalista toiminnastaan, mutta se ilmoittaa poikkeavasta toiminasta hälytyksinä. Haasteena tässä on, että se voi tehdä vääriä hälytyksiä liian paljon. Toisena ongelmana on löytää dataa opettamiseen, josta ei seuraisi onnistuneita hyökkäyksiä. Kolmas nostetteva ongelma on se, että hyökkääjä pystyy pikkuhiljaa opettamaan järjestelmää pitämään haitallista liikennettä normaalina, jonka myötä hyökkäykset onnistuvat. (Sommer ja Paxson, 2010.)

4 Tekoälyn soveltaminen hajautetun palvelunestohyökkäysten havaitsemisessa

Tässä kappaleessa käsitellään tekoälyn mahdollisuuksista hajautettujen palveluestohyökkäysten havaitsemisessa. Kappaleessa lisäksi vertaillaan keskinäisiä havaitsemiskyvykkyysien tuloksia. Lopuksi käydään läpi haasteita, mitä tekoäly voi tuoda hajautettujen palvelunestohyökkäysten havaitsemisessa.

4.1 Tekoälyn mahdollisuudet hajautetun palvelunestohyökkäysten havaitsemisessa

Alghoson ym. (2021) kertoivat tekoälyn ja tarkemmin koneoppimisen mallien käytöstä DDoS-hyökkäysten torjumisessa. Tässä kyseisessä tieteellisessä artikkelissa kokeiltiin erilaisia koneoppimisen algoritmeja SDN-ympäristössä (Alghoson ym., 2021).

Yksi näistä algoritmeista oli satunnaismetsä, joka muodostaa koulutusvaiheessa suuren määrän päätöspuita ja samalla luo luokan, joka yhdistää näiden tuloksen (Alghoson ym., 2021). Yang ja Chen (2016) avasivat, mikä päätöspuu algoritmi on. Päätöspuu on koneoppimismalli, jolla on juuripohjamainen rakenne. Tässä rakenteessa edetään solmuja pitkin, jotka edustavat päätöksentekoa ja näillä aineisto voidaan jakaa alakategorioihin. Tässä rakenteessa lehtisolmut ovat sitten näitä päätöksiä, mihin päädytään lopullisesti päätöspuissa. (Yang ja Chen, 2016.) Tämän päätöspuu kaltaisen rakenteen vuoksi, sitten satunnaismetsä algoritmin tulos on vakaa ja erityisen tarkka. Toinen nopeasti toimiva algoritmi on Light Gradien Boostin eli LightGBM on gradienttiboostausmenetelmä, joka toimii myös perustuen päätöspuihin. Tämä algoritmi jakaa puun lehtikohtaisesti, mikä tarkoittaa, että se valitsee parhaan sopivuuden jokaiselle lehdelle erikseen kasvattamatta koko puun syvyyttä tasaisesti. Toiset boostausalgoritmit kasvattavat taas koko puun syvyyttä tasaisesti. CatBoost algoritmi on myös gradienttiboostausmenetelmä, joka myös perustuu päätöspuihin, joka on helposti integroitavissa syväoppimisarkkitehtuuriin. Se pystyy käsittelemän useita eritietotyyppejä ja sen voiksi erinomainen ongelmien ratkaisija. Viimeinen käytetty algoritmi on Convolutional Neural Network (CNN), joka on syväoppimisverkko. Tässä CNN:ssä jokaisen kerroksen neuroni on yhdistetty seuraavan kerroksen kaikkiin neuroneihin, joka hyödyntää konvoluutio-operaatiota. Tämän vuoksi voidaan havaita piirteitä datasta erityisellä lineaarisella operaatiolla. (Alghoson ym., 2021.)

Tässä tutkimuksessa käytettiin tekoälyn koulutukseen CICDDoS2019-datajoukkoa. Tämän opetusmateriaalin kautta todettiin satunnaismetsä olevan tarkin algoritmi havaita DDoS-hyökkäyksiä jopa 99,9974 % tarkkuudella. (Alghoson ym., 2021.)

Haider ym. (2020) kertoivat SDN-ympäristössä syväoppimisen käyttöä DDoS-hyökkäysten havaitsemiseen. Tässä tutkimuksessa havaittiin parhaaksi

syväoppimismalliksi konvulaatioverkot ja tarkemmin CNN, joka käytti CICIDS2017-opetusdataa ja saaden 99,48 % tarkkuuden. (Haider ym., 2020.)

Chavan ym. (2022) käsittelivät koneoppismallien käyttöä DDoS-hyökkäysten havaitsemiseen. Eräs niistä oli K-Nearest Neightbors eli KNN, jossa algoritmi luokittelee tai ennustaa käyttäen lähiempien havaintojoukon ominaisuuksia ja tämän avulla osaa tehdä uuden ennusteen. KNN on tehokas, kun datan rakenne tukee tätä lähestymistapaa. Toinen malli on Logistinen regressio, joka on tarkoitettu binääriseen luokitteluun. Algoritmin ennustemuuttujan ja riippumattomien muuttujien välistä yhteyttä pyritään tutkimaan ja algoritmi muuntaa todennäköisyydet sigmoidifunktion avulla arvoiksi välillä 0 ja 1, jotta voidaan luokitella, mikäli on hyökkäys vai ei. Tukivektorikone eli SVM oli myös käytössä tässä, joka pyrkii etsimään hypertasoa, joka olisi optimaalinen erottamaan luokat toisistaan mahdollisimman selkeästi. SVM pystyy toimimaan monimutkaisissa ja moniulotteisissa aineisteistoissa. Tutkielman myös käytettiin päätöspuita, mutta parhaan tuloksen NSL-KDD-opetusdatan kanssa logistinen regressio sai 90,4 % DDoS-hyökkäysten havaitsemisesta. (Chavan ym., 2022.)

Plazas Olaya ym. (2023) pohtivat, miten koneoppimismallien käyttöä voidaan myös hyödyntää DDoS-hyökkäyksiä vastaan IoT-laitteissa eli fyysisissä laitteissa, joissa on jotakin sensoreita tai ohjelmistoja, joka mahdollistaa datan keräyksen ja vaihdon. Koneoppimismallit pystyvät vähentämään viivettä ja mahdollistaa nopean DDoS-hyökkäysten havaitsemisen. Tässä tutkimuksessa käytettiin päätöspuita, satunnaismetsää, logistista regressiota ja tukiverkkokonetta. Opetusdatana käytettiin BoT-IoT ja UNSW-NB15 yhdistelmää ja parhaan tuloksen sai satunnaismetsä 99,9989 %, mutta kaikki muutkin saivat 99,99 % tuloksen. (Plazas Olaya ym., 2023.)

Hussain ym. (2020) kertovat, miten syväoppimismallit myös sopivat DDoS-hyökkäyksiä havaitsemisessa IoT-ympäristössä. CNN-verkkopohjainen ResNet eli Residual Network on suunniteltu käyttämään kuvantunnistustehtävissä, mutta se toimii myös DDoS-hyökkäysten havaitsemisessa, sillä se pystyy muuttamaa tietoliikenne datan kuviksi. ResNet pystyy ohittamaan tiettyjä kerroksia, joka edistää syvien neuroverkkojen hitaampaa oppimista ja tämän vuoksi on suorituskyvykäs. DDoS-hyökkäysten havaitsemiseen käytettiin CICDDoS2019-opetusdatana.

Tekoälyä ja tarkemmin ottaen koneoppimista voidaan käyttää pilvipalvelujen DDoS-hyökkäyksin torjumisessa. Pilvipalvelut ovat internetin välityksellä olevia tietokone- ja verkkopalveluja, joita voidaan käyttää etänä ilman omia fyysisiä resursseja, joista maksetaan niistä palveluista vastaaville. SaE-ELM on neuroverkkomallin, sekä evoluutiomenetelmänyhdistelmä ja tarkemmin ottaen differentiaalievoluutio voidaan käyttää tässä pilvipalveluympäristössä DDoS-hyökkäysten havaitsemiseen. Tämä differentiaalievoluutio toiminta perustuu siihen, että ratkaisu joukkoa parannetaan sukupolvien eli ajan myötä. SaE-ELM (Self-adaptive evolutionary extreme learning machine) toiminta yhdistää nämä neuroverkkojen nopeat laskentamenetelmät ja evoluutioalgoritmien kokemuksen myötä tulevan optimoinnin. Tämä SaE-ELM onnistui havaitsemaan DDoS-

hyökkäyksiä CICIDS 2017-opetusdataa käyttäen 99,99 % tarkkuudella. (Kushwah ja Ranga, 2021.)

Dendriittisolualgoritmi eli DCA pystytään myös käyttämään DDoS-hyökkäysten havaitsemisessa. Se pyrkii havaitsemaan ja luokittelemaan soluissaan soluagenttien avulla verkkoliikennettä tunnistaen, mitkä ovat normaaleja turvallisia signaaleja ja mitkä ovat vaarasignaaleja. Tällä algoritmi tekniikalla päästiin 98,6 % tarkkuuteen NSL-KDD-opetusdataa käyttäessä. (Igbe ym., 2017.)

4.2 Tutkimusten vertailu

Taulukkossa 1 on esitelty eri tekoälymenetelmien DDoS-hyökkäysten havaitsemistarkkuudet. Alghoson ym. (2021) ja Plazas Olaya ym. (2023) tutkimuksissa koneoppimismallit olivat merkittävän tarkkoja ja erityisesti tämä satunnaismetsä algoritmit, joilla havaitaan DDoS-hyökkäyksiä. Chavan ym. (2022) eivät päässeet siis yhtä hyviin tuloksiin kuin mihin Plazas Olaya ym. (2023) ja Alghoson ym. (2021) pääsivät koneoppimista käyttäen. Erityisesti Chavan ym. (2022) saamat tulokset havaitsemisesta jäivät vajaiksi.

Syväoppimismalleissa ja niiden kyvykkyyksissä havaita DDoS-hyökkäyksiä oli eroavaisuuksia Haider ym. (2020), Kushwah ja Ranga (2021) ja Hussain ym. (2020) välillä. Hussain ym. (2020) sekä Kushwah ja Ranga (2021.) saivat metodeillaan kumminkin yli 0,5 % paremman tuloksen kuin Haider ym. (2020).

Igbe ym. (2017) Dendriittisolualgoritmi havaitsemiskyky ei suoriutunut, mitenkään erityisen hyvin, kun vertaa Plazas Olaya ym. (2023) koneoppimismallien tuloksiin tai Hussain ym. (2020) syväoppimismallien tuloksiin. Igbe ym. (2017) algoritmi suoriutuu kuitenkin silti selkeästi paremmin, kuin Chavan ym. (2022) logistinen regressio.

Taulukko 1 esittelee eri tekoälymenetelmien DDoS-hyökkäysten havaitsemistarkkuudet. Tämä kyseinen taulukko tiivistää keskeisiä tutkimustuloksia.

TAULUKKO 1 Erilaisten tekoälymenetelmien DDoS-hyökkäysten havaitsemistarkkuus.

Menetelmä	Opetusdata	Havaitsemistarkkuus
Satunnaismetsä (Alghoson ym., 2021)	CICDDoS2019 (Alghoson ym., 2021)	99,9974 % (Alghoson ym., 2021)
CNN (Haider ym., 2020)	CICIDS2017 (Haider ym., 2020)	99,48 % (Haider ym., 2020)
Logistinen regressio (Chavan ym., 2022)	NSL-KDD (Chavan ym., 2022)	90,4 % (Chavan ym., 2022)
Satunnaismetsä (Plazas Olaya ym., 2023)	BoT-IoT ja UNSW-NB15 yhdistelmä (Plazas Olaya ym., 2023)	99,9989 % (Plazas Olaya ym., 2023)
ResNet (Hussain ym., 2020)	CICDDoS2019 (Hussain ym., 2020)	99,99 % (Hussain ym., 2020)

SaE-ELM (Kushwah ja Ranga, 2021)	CICIDS 2017 (Kushwah ja Ranga, 2021)	99.99 % (Kushwah ja Ranga, 2021)
DCA (Igbe ym., 2017)	NSL-KDD (Igbe ym., 2017)	98,6 % (Igbe ym., 2017)

4.3 Tekoälyyn perustuvien ratkaisujen haasteet

Doriguzzi-Corin ym. (2020) totesivat artikkelissaan, että tekoäly ja tarkemmin ottaen syväoppimisen CNN pystyy tarjoamaan korkean tasoisia tuloksia DDoS-hyökkäysten havaitsemisessa. Tässä kumminkin haasteen voi tulla vastaan, kun tätä metodia kokeillaan rajoitetumpien resurssien ympäristössä ja halutaan samalla ylläpitää tätä saman tasoluokan tarkkuutta. (Doriguzzi-Corin ym., 2020.)

Banitalebi Dehkordi ym. (2021) kertoivat ongelmasta, mikäli käytetään vanhaa dataa koneoppimismalleissa DDoS-hyökkäysten havaitsemiseen. Tämä johtaa siihen, että mallin kyvykkyys havaita hyökkäyksiä nopeasti hidastuu, koska se heikentää mallin joustavuutta havaita uusia hyökkäyksiä (Dehkordi Dehkordi ym., 2021). Ortet Lopes ym. (2021) totesivat myös tähän liitteyn, että nykyisistä syväoppimisen malleista suurin osa ei pysty havaitsemaan nykyisiä DDoS-hyökkäyksiä, mallien koulutusaineistojen rajoittuneisuuksien takia.

5 Yhteenveto

Tämän tutkielman pääteemat olivat tekoäly ja DDoS-hyökkäykset. Päätavoitteena tutkielmassa oli selvittää vastaus tutkimuskysymykseen, joka oli seuraavanlainen: *miten tekoälyä voitaisiin hyödyntää hajautettujen palveluestohyökkäysten havaitsemisessa tekoälyä?* Tutkimus suoritettiin kirjallisuuskatsauksena, joka lähti liikkeelle tekoälyn määritelmästä ja -kehityskaaresta. Tutkielmassa tuotiin esille tekoälyn erilaisia menetelmiä, sekä lisäksi käsiteltiin tekoälyyn liittyviä vahvuuksia ja heikkouksia. Lisäksi tutkielmassa käsiteltiin tekoälymenetelmien mahdollisuuksista kyberturvallisuuden kontekstissa. Tutkielmassa esiteltiin DDoS-hyökkäysten eri tyyppejä ja DDoS-hyökkäysten tuomia vaikutuksia. Tämän lisäksi käsiteltiin DDoS-hyökkäysten perinteisiä havaitsemisen menetelmiä ja niihin liitettäviä haasteita. Nämä aiheet myös yhdistettiin, jolloin päästiin käsittelemään tutkielman pääteemaa eli, miten tekoäly toimii DDoS-hyökkäysten havaitsemisessa. Tutkielmassa pyrittiin selvittämään, kuinka tarkasti eri tekoälyteknologiat toimivat DDoS-hyökkäysten havaitsemisessa, mutta myös siihen liittyviä mahdollisia haasteita.

Tässä kirjallisuuskatsauksessa käytettiin lähteiden hakuun pääasiassa seuraavia hakupalveluita: JYUDOK, Google Scholar, IEEE Xplore ja Springer. Lähteitä haettiin yhdistellen seuraavia sanoja kuten "DDoS", "Artificial Intelligence" ja "distributed denial of service detection". Lähdeaineiston haussa on pyritty huomioimaan lähteiden tuoreutta, ja useimmat lähteistä ovat 2020-luvulta.

Kyberhyökkäykset kehittyvät jatkuvasti, minkä vuoksi nykyaikana vaaditaan aiempaa tehokkaampia puolustusmenetelmiä. Tähän liittyen Khalaf ym. (2019) totesivat, että DDoS-hyökkäysten havaitsemiseen ei riitä enää perinteiset menetelmät, ja tekoäly voisi olla ratkaisu tähän. DDoS-hyökkäykset pystyvät kuitenkin merkittäviin tuhoin, kuten Hanner ja Knake (2021) kertoivat Virossa suuren DDoS-hyökkäyksen aiheuttamasta taloudellisista menetyksistä ja jopa ihmisten heikentyneestä uskosta hyökkäyksien kohteena olleisiin instituutioihin. Tämän vuoksi aihe on merkittävä, että löydettäisiin mahdollisia ratkaisuja ongelmaan ja vältyttäisiin jopa näin suurilta DDoS-hyökkäyksien tuhoilta tulevaisuudessa.

Tutkielmassa käytetyt DDoS-hyökkäysten havaitsemismenetelmät toivat eritasoisia tuloksia. Algoritmit pystyivät tuottamaan jopa erityisen tarkkoja tuloksia, kuten Alghoson ym. (2021) ja Plazas Olaya ym. (2023) satunnaismetsä, Hussain ym. (2020) ResNet ja Kushwah ja Ranga (2021), jotka kaikki saivat 99,99 % tuloksen. Chavan ym. (2022) Logistinen regressio sai taas vastaavasti heikomman tuloksen, joka oli 90,4 %.

Kirjallisuuskatsauksessa hyödynnettyjen lähteiden perusteella vastauksena tutkimuskysymykseen voidaan todeta, että tekoälyä on mahdollista käyttää monin eri menetelmin DDoS-hyökkäysten havaitsemiseen, jopa erityisen tarkasti. Kuitenkin kaikki tekoälymenetelmien algoritmit eivät ole riittävän tarkkoja, minkä vuoksi tulee pohtia niiden käytettävyyttä, jotta havaitsemistarkkuus ei jäisi heikoksi. On myös tärkeää huomioida, että käytettävä algoritmi on

ympäristöön sopiva ja, että tämän opetusdata on tarpeeksi tuoretta havaitsemaan nykyisiä DDoS-hyökkäyksiä.

Vaikka tutkimuksessa pystyttyiin tuomaan esiin merkittäviä havaintoja tekoälyn mahdollisuuksista DDoS-hyökkäyksien havaitsemisessa, on tärkeää huomioida tutkimuksen rajoittuneisuus. Tutkimus oli kirjallisuuskatsaus, eikä tuottanut uutta empiiristä dataa. Tutkimuksen tuottamat tulokset jäivät melko yleiselle tasolle eikä tuotu esille, miten niitä voitaisiin käyttää konkreettisesti. Tutkimuksessa esille tuodut havaitsemismenetelmät eivät käyttäneet samoja opetusdatoja, joten on huomioitava, että havaitsemistarkkuudet voisivat tuottaa erilaisia tuloksia samoilla opetusdatoilla.

DDoS-hyökkäysten havaitsemismenetelmien opetukseen käyttämät opetusdatat eivät olleet samoja, minkä vuoksi havaitsemismenetelmät eivät olleet samalla lähtöviivalla. Tämän takia jatkotutkimuksena voisi kehittää empiirisen tutkimuksen, jossa testattaisiin eri tekoälymenetelmien tarkkuutta samanlaisessa ympäristössä. Tutkimukseen voisi liittää myös saman opetusdatan käytön kaikille menetelmille ja tuoda esille, miten havaitut menetelmät voitaisiin tuoda konkreettisesti käyttöön. Tällä tutkimuksella voitaisiin testata, mikä olisi tarkin menetelmä DDoS-hyökkäysten havaitsemiseen ympäristöstä riippumatta. Tällöin menetelmät olisivat samalla lähtöviivalla.

LÄHTEET

Abhishta, S., Joosten, R., & Nieuwenhuis, L. J. M. (2017). Analysing the impact of a DDoS attack announcement on victim stock prices. *2017 25th Euromicro International Conference on Parallel, Distributed and Network-Based Processing,* 354–359. IEEE. https://doi.org/10.1109/PDP.2017.82

Abu Bakar, R., Huang, X., Javed, M. S., Hussain, S., & Majeed, M. F. (2023). An intelligent agent-based detection system for DDoS attacks using automatic feature extraction and selection. *Sensors,* 23(6), 3333. https://doi.org/10.3390/s23063333

Alghoson, E. S., & Abbass, O. (2021). Detecting distributed denial of service attacks using machine learning models. *International Journal of Advanced Computer Science and Applications,* 12(12), 616–622. https://doi.org/10.14569/IJACSA.2021.0121277

Asad, M., Asim, M., Javed, T., Beg, M. O., Mujtaba, H., & Abbas, S. (2020). DeepDetect: Detection of distributed denial of service attacks using deep learning. *The Computer Journal,* 63(7), 983–994. https://doi.org/10.1093/comjnl/bxz064

Awan, M. J., Farooq, U., Babar, H. M. A., Yasin, A., Nobanee, H., Hussain, M., Hakeem, O., & Zain, A. M. (2021). Real-time DDoS attack detection system using big data approach. *Sustainability*, 13(19), 10743. https://doi.org/10.3390/su131910743

Banitalebi Dehkordi, A., Soltanaghaei, M. R., & Zamani Boroujeni, F. (2021). The DDoS attacks detection through machine learning and statistical methods in SDN. *The Journal of Supercomputing,* 77(3), 2383–2415. https://doi.org/10.1007/s11227-020-03323-w

Brooks, R. R., Yu, L., Ozcelik, I., Oakley, J., & Tusing, N. (2021). Distributed denial of service (DDoS): A history. *IEEE Annals of the History of Computing,* 44(2), 44–53. https://doi.org/10.1109/MAHC.2021.3072582

Chavan, N., Nishad, N., Kukreja, M., Deb, N., & Jagwani, G. (2022). DDoS attack detection and botnet prevention using machine learning. *2022 8th International Conference on Advanced Computing and Communication Systems (ICACCS),* 1159–1163. IEEE. https://doi.org/10.1109/ICACCS54159.2022.9785247

Dinmohammadi, F. (2023). Adopting artificial intelligence in Industry 4.0: Understanding the drivers, barriers, and technology trends. *Proceedings of the 28th International Conference on Automation & Computing*. IEEE. https://doi.org/10.1109/ICAC57885.2023.10275230

Doriguzzi-Corin, R., Millar, S., Scott-Hayward, S., Martínez-del-Rincón, J., & Siracusa, D. (2020). Lucid: A practical, lightweight deep learning solution

for DDoS attack detection. *IEEE Transactions on Network and Service Management*, 17(2), 876–889. https://doi.org/10.1109/TNSM.2020.2971776

Elubeyd, H., & Yiltas-Kaplan, D. (2023). Hybrid deep learning approach for automatic DoS/DDoS attacks detection in software-defined networks. *Applied Sciences,* 13(3828). https://doi.org/10.3390/app13063828

Falowo, O. I., Okpala, I., Kojo, E., Azumah, S., & Li, C. (2023). Exploration of various machine learning techniques for identifying and mitigating DDoS attacks. *20th Annual International Conference on Privacy, Security and Trust (PST).* IEEE. https://doi.org/10.1109/PST58708.2023.10320151

Haider, S., Akhunzada, A., Ahmed, G., & Raza, M. (2019). Deep learning based ensemble convolutional neural network solution for distributed denial of service detection in SDNs. *2019 4th International Conference on Emerging Technologies (ICET).* IEEE. https://doi.org/10.1109/UCET.2019.8889027

Haner, J. K., & Knake, R. K. (2021). Breaking botnets: A quantitative analysis of individual, technical, isolationist, and multilateral approaches to cybersecurity. *Journal of Cybersecurity, 7*(1), Article tyab003. https://doi.org/10.1093/cybsec/tyab003

Hussain, F., Abbas, S. G., Husnain, M., Fayyaz, U. U., Shahzad, F., & Shah, G. A. (2020). IoT DoS and DDoS attack detection using ResNet. *2020 IEEE 23rd International Multitopic Conference (INMIC).* IEEE. https://doi.org/10.1109/INMIC50486.2020.9318216

Igbe, O., Ajayi, O., & Saadawi, T. (2017). Denial of service attack detection using dendritic cell algorithm. *2017 IEEE International Conference on Cyber Security and Cloud Computing*. IEEE. https://doi.org/10.1109/CSCloud.2017.294

Jiang, Y., Li, X., Luo, H., Yin, S., & Kaynak, O. (2022). Quo vadis artificial intelligence? *Discover Artificial Intelligence, 2*(4). https://doi.org/10.1007/s44163-022-00022-8

Kalutharage, C. S., Liu, X., Chrysoulas, C., Pitropakis, N., & Papadopoulos, P. (2023). Explainable AI-based DDoS attack identification method for IoT networks. *Computers, 12*(2), 32. https://doi.org/10.3390/computers12020032

Kaur, P., Kumar, M., & Bhandari, A. (2017). A review of detection approaches for distributed denial of service attacks. *Systems Science & Control Engineering: An Open Access Journal, 5(*1), 301–320. https://doi.org/10.1080/21642583.2017.1331768

Khalaf, B. A., Mostafa, S. A., Mustapha, A., Mohammed, M. A., & Abduallah, W. M. (2019). Comprehensive review of artificial intelligence and statistical approaches in distributed denial of service attack and defense methods. *IEEE Access, 7*, 51691–51733. https://doi.org/10.1109/ACCESS.2019.2908998

Kushwah, G. S., & Ranga, V. (2021). Optimized extreme learning machine for detecting DDoS attacks in cloud computing. *Computers & Security, 105*, 102260. https://doi.org/10.1016/j.cose.2021.102260

LeCun, Y., Bengio, Y., & Hinton, G. (2015). Deep learning. *Nature, 521*(7553), 436–444. https://doi.org/10.1038/nature14539

Nuiaa, R. R., Manickam, S., & Alsaeedi, A. H. (2021). Distributed reflection denial of service attack: A critical review. *International Journal of Electrical and Computer Engineering, 11*(6), 5327–5341. https://doi.org/10.11591/ijece.v11i6.pp5327-5341

Osterweil, E., Stavrou, A., & Zhang, L. (2020). 21 years of distributed denial-of-service: Current state of affairs. *Computer, 53*(7), 88–92. https://doi.org/10.1109/MC.2020.2983711

Russell, S. J., & Norvig, P. (2010). *Artificial intelligence: A modern approach* (3rd ed.). Prentice Hall. ISBN-13: 978-0-13-604259-4

Sarker, I. H. (2021). Machine learning: Algorithms, real-world applications and research directions. *SN Computer Science, 2*(160). https://doi.org/10.1007/s42979-021-00592-x

Sommer, R., & Paxson, V. (2010). Outside the closed world: On using machine learning for network intrusion detection. *2010 IEEE Symposium on Security and Privacy*, 305–316. IEEE. https://doi.org/10.1109/SP.2010.25

Yang, Y., & Chen, W. (2016). Taiga: Performance optimization of the C4.5 decision tree construction algorithm. *Tsinghua Science and Technology, 21*(4), 415–425. https://doi.org/10.1109/TST.2016.7570085