NETWORK ANOMALY DETECTION WITH MACHINE LEARNING

HÁLÓZATI ANOMÁLIÁK DETEKTÁLÁSA GÉPI TANULÁSSAL

NAGY ATTILA[1]

Abstract

Information security is becoming increasingly important these days. Computer network security includes virus scanners, firewalls, intrusion detectors. Intrusion detection systems are being developed year after year. Research with deep learning and quantum computers is being done these days. These two areas have become popular research areas. Intrusion detectors have become faster and more accurate. In this paper, I present what elements are needed to detect network anomalies in computer networks using machine learning models. And finally, we touch on the quantum computer.

Keywords

Network, anomaly, machine learning, deep learning

Absztrakt

Napjainkban egyre fontosabb az információ biztonság. A számítógépes hálózat biztonsághoz tartoznak a vírusírtók, tűzfalak, behatolás érzékelők. A behatolás érzékelő rendszereket évről évre fejlesztik. A mélytanulás és a kvantum számítógépekkel végeznek napjainkban kutatásokat. Ez a két terület népszerű kutatási terület lett. A behatolás érzékelők gyorsabbak, pontosabbak lettek. A tanulmányban bemutatom milyen elemek szükségesek, hogy a számítógépes hálózatokban észlelni tudjuk a hálózati anomáliákat gépi tanulási modellekel. Végezetül a kvantum számítógépet is érintjük.

Kulcsszavak

Hálózatok, anomáliák, gépi tanulás, mélytanulás

[1] Nagy.a@uni-obuda.hu | ORCID: 0000-0003-0214-414X | PhD Student, Óbuda University Doctoral School for Safety and Security Sciences | doktorandusz, Óbudai Egyetem Biztonság-tudományi Doktori Iskola

BEVEZETÉS

A számítógépes hálózat védelme a 21. században egy fontos feladattá nőte ki magát. A nemzetek az információs társadalom kialakításában tevékenykednek. Az ilyen társadalmakban a mindennapi élet részét képezi az információ, a kommunikáció és a tudás. A modern kor információs forradalmat többféle képen lehet jellemezni: a digitális elektronika megjelenése, az informatikai eszközök térhódítása, ezen belül a számítógépes hálózatok fejlődése, a tudomány rohamos fejlődése és terjeszkedése és még a tudásipar és multimédia megjelenése stb. Mint láthatjuk a számítógépes hálózat szerves része az információs forradalomnak. [1] 1995. decemberében az internethasználók száma 16 millió volt. 2021 márciusára ez a szám 5.1 milliárdra ugrott, ami a Föld lakosságának 56,6% teszi ki. [2] Európában az internetfelhasználók száma a Föld lakosságának 14.2% teszi ki. [3] A KSH adatai alapján Magyarországon a 2020-as évben az internethasználók aránya 85% volt. [4] Az internetre csatlakozott internet of things (IoT) eszközök száma 2019-ben 7.74 milliárd volt, 2022-re ez a szám 11.57 milliárdra ugrott és 2030-ra 25.44 milliárd eszközt jósolnak a szakértők. [5] Az adatokból látható, hogy a hálózatok napról napra terjednek méretben és komplexitásban egyaránt. A terjedéssel a támadási felülete is megnő az infrastruktúrának. A számítógép-hálózatok védelmének megvalósítása lehet passzív és aktív. Az Európai Uniós kiberbiztonsági ügynökség (ENISA) 2021-ben az évente kiadott jelentésében, nyolc kiberbiztonsági fenyegetettséget emeltek ki. Zsarolóvírus (ransomware): a kártékony szoftverek családjába tartozik. A támadás az áldozat adatait rejtjelezi és csak pénz ellenében fejtik vissza az adatokat, rosszindulatú szoftverek (malware) vagy kártékony szoftverek egy gyűjtőnév, ami magában foglalja a vírusokat, férgeket, kémszoftvereket stb. A cryptolopás (cryptojacking) vagy rejtett kriptobányászat egy olyan bűncselekmény, ami az áldozat számítógép erőforrásait felhasználva a bűnözőnek hoz hasznot, e-mail-el összefüggő fenyegetések (E-mail related threats) az ide tartozó fenyegetések a phishing, spear-phishing, whaling, smishing, bishing, spam. A fenyegetések az adatok ellen (threats agains data) olyan fenyegetések gyűjteménye, ami az adatok ellen irányul azzal a céllal, hogy jogosulatlan hozzáférést, nyilvánosságra hozatalt szerezzenek. A fenyegetettségek a rendelkezésreállás és a sértetlenség ellen (threats against availability and integrity): a rendelkezésreállásra irányuló támadás az elosztott szolgáltatás-megtagadással járó (DDoS) támadással támadják. Dezinformáció és félretájékoztatás (disinformation - misinformation): a dezinformáció egy szándékos támadás, amely hamis vagy félrevezető információk létrehozásából vagy megosztásából áll. Ez a típusú támadás a COVID-19 pandémia idején exponenciálisan megnövekedtek (pl. az oltás manipulálására használták). A félretájékoztatás nem szándékos támadás. Ebben az esetben az információ megosztása véletlenül történik (pl. az újságíró rossz információról számol be). Minden információ hordozhat magában pontatlan részeket. A nem rosszindulatú fenyegetettségek (non-malicious threats): álltalában emberi hibára vagy hibás beállításra alapoz a támadás. [6] A számítógép-hálózatok védelmének megvalósítása lehet passzív és aktív. Passzív lehet: tűzfal, vírusirtó, hozzáférési szabályozás, behatolás detektálás. Az aktív védelem lehet: megelőző támadás, ellentámadás és aktív megtévesztés. Az említett fenyegetettségeket a számítógépes hálózat forgalmában észlelhető különböző megoldásokkal. Az egyik megoldás a behatolás érzékelő rendszer. A mai technológia fejlettség mellet a klasszikus behatolás érzékelő rendszerek elavultak mivel lassúak, sok fals negatív riasztás jeleznek be és a null-napi támadások ellen sem hatékonyak mivel nem ve-

szik észre a fenyegetést. 2014-ben a mély tanulás megjelenésével esélyünk lett a gépi tanulási algoritmusokkal új behatolás érzékelőket fejleszteni és használni. A régi behatolás érzékelőkkel szemben az új módszerrel a sebessége megnő, precízebb lesz és az ismeretlen támadásokat (null-napi támadások) is felismeri, amivel egy érzékenyebb rendszert fogunk kapni. Ha nem lenne elég a klasszikus számítógépek gyorsasága akkor a nem túl távoli jövőben megjelennek a kvantum számítógépek, ami az észlelő képesség gyorsaságán fog javítani. A következő néhány oldalban a behatolás rézkelő rendszerek fontosabb elemeit részletezzük.

Behatolásérzékelő rendszerek

A behatolásérzékelő rendszer gondolatával először Dorothy Denning és Peter Neumman játszott el. Ők fejlesztették ki 1984 és 1986 között az első valós idejű behatolásérzékelő rendszert (angol nevén: Intrusion Detection System – IDS). A behatolásérzékelő rendszereket két csoportra lehet bontani, host-alapú behatolásérzékelő rendszerre és hálózatalapú behatolásérzékelő rendszerre. A host-alapú rendszer log és állományok monitorozására használják. A hálózatalapú rendszereket pedig a hálózatok monitorozására használják, ami számunkra fontos. A hálózatalapú behatolásérzékelő rendszerek két fő modellt alkalmaznak az észlelésre (rendellenességet észlelő modell és visszaélést érzékelő modell). A rendellenességet észlelő modellhez tartozik az anomália alapú, viselkedés alapú és irányelv alapú észlelés. A visszaélést érzékelő modellnél pedig a tudáson alapúló és helytelen használatra alapúló észlelés használja. [7]

Gépi tanulás

A gépi tanulás térhódítása azért lehetséges mert a 21. században rengeteg adatot gyűjtöttünk és nagy teljesítményű számítógépeket is fejlesztettünk ki. Ennek segítségével a gépi tanulási algoritmusokat képesek vagyunk alkalmazni és olyan kapcsolatokat találhatunk az adatok között, amit máshogy nem lennénk képesek észlelni sem szemmel, sem más eszközökkel. Az 1950-es években jelentek meg az első algoritmusok csak akkor még nem tudtuk őket használni adat és hardware hiánya miatt. A gépi tanulási algoritmusokat fel lehet osztani tanulásuk szerint, ebben az esetben három fő csoportot kapunk (felügyelt tanulás, felügyelt nélküli tanulás és megerősítéses tanulás). Ha a hálózatokban szeretnénk észlelni az anomáliákat akkor a felügyelt nélküli tanulást kell alkalmazni. A felügyelt nélküli tanuláshoz tartoznak a következő algoritmusok: K-közép, SVD mint dimenzió csökkentő, Gauss mátrix, neurális hálózatok és a neurális hálózatokból kifejlődött mély tanulás, amit 2010-ben kezdtek az emberek használni. [8]

Neurális hálózat

A neurális hálózat az emberi agy működését próbálja leutánozni. A neuronok együttműködő processzáló elemek melyek számításokat végeznek el. Ezek a neuronok ún. rétegekből épülnek fel. Az információ csak rétegből rétegre halad egy irányba a bemeneti rétegből a kimeneti rétegig vagy a kimeneti rétegtől a bemenet felé terjed. [8]

Mély tanulás

A mély tanulás a gépi tanulás mesterséges neurális hálózatokon alapuló alkészlete. A tanulási folyamat azért mély mert a neurális hálózatok struktúrája több bemenetet, kimenetet és rejtett réteget tartalmaz. Az összes réteg egységekből épülnek fel, melyek a bemeneti információt úgy alakítja át, hogy a következő réteg eltudja végezni a predektív feladatot. [9]

A kiberbiztonság területén a gépi tanulást, mint módszert több területen lehet alkalmazni. Kártevő alkalmazások észlelésére, az emberi manipuláció detektálására ide tartozik a deepfake, a dezinformáció, személyazonosság analízise. A behatolás észleléshez tartoznak a webszerverek sérülékenysége, a tor hálózaton nyomon követni egyes felhasználót vagy kártevő weboldalak detektálására. Az automatikus behatolás detektáláshoz az adathalász oldalak érzékelése és a hálózati anomáliák észlelése tartozik. [10] A gépi tanulás széleskörű felhasználási lehetőséget nyújt a kiberbiztonság területén is. A továbbiakban az anomáliák detektálásával fogunk foglalkozni.

A gépi tanulási algoritmusokat számos területen alkalmazható, a kiberbiztonság területén egyaránt. A gépi tanulási algoritmusok üzemanyaga az adat. Ezek az adatok adatkörökbe vannak szedve. A mi esetünkben az adatkörök hálózati forgalmat tartalmaznak neutrális és káros adatokat egyaránt, aminek segítségével a gépi tanulási algoritmusok képesek mintákat találni és a hasznos adatforgalmat eltudja különíteni a káros adatforgalomtól.

Adatkörök

A hálózati forgalmat tartalmazó adatkörök beszerzése régen nehéz volt. A hálózati adatforgalom nem publikus ez miatt nem volta egyszerű a beszerzése. Az egyik Kanadai Intézet ami kiberbiztonsággal foglalkozik évről évre újabb és újabb adatköröket készített (pl. Intrusion detection system 2018 vagy a 2017es változat, Túlterhelésestámadási adatköröket is készítettek, Darknet, TOR és VPN adatköröket is). A minőséges kutatáshoz ez nem kielégítő. A tanulmányban mi az IDS 2018-as változatát választottuk mivel ez a legújabb. Az adatkör a következő támadásokat tartalmazza: [11]

- Nyers erő támadás más néven bruteforce támadás (FTP, SSH)
  Az ilyen féle támadással a behatoló kevés információval rendelkezik az áldozatról és úgy próbálja megkerülni a biztonsági védelmet, hogy nyers erő támadást alkalmaz, ami azt jelenti, hogy egy megadott csoportú karakterekkel próbál a jelszóra rájönni. Ha a jelszú gyenge akkor eredményes tud lenni az ilyen féle támadás. [12]
- Szolgáltatásmegtagadó támadás (Slowloris, GoldenEye, Hulk, Slowhttp)
- Webalapú támadás (Nyers erő támadás, xss és DVWA)
  Az XSS vagy Cross site scripting egy számítógépes sebezhetőség, amely webalkalmazásoknál fordul elő. A támadó egy olyan kódot illeszt be a weboldalra, amit minden felhasználó lát. Ez lehet egy HTML kód is. Ha felfedezünk egy XSS sérülékenységet akkor kikerülhetjük a hozzáférési ellenőrzéseket pl. úgy, hogy nem a weblapról számozó eredeti forrást használjuk fel. Napjainkban ezt a támadást az adathalász támadás végrehajtásánál alkalmazzák. [13]
- Zombi hálózat támadás
  „A kiberbűnözők által menedzselt botneteket, olyan internetes kapcsolattal rendelkező szoftver robotok, ún. zombi számítógépek alkotják, amelyeket a gépen futó

valamely program sebezhetőségét kihasználva távolról megfertőznek, vagyis amelyekre valamilyen távoli menedzselésre is alkalmas rosszindulatú programot telepítenek a felhasználó tudta és akarata nélkül" [14]
- Beszivárgó támadás
- Port letapogatás és elosztott túlterheléses támadás (http kérés, LOIC) [11]

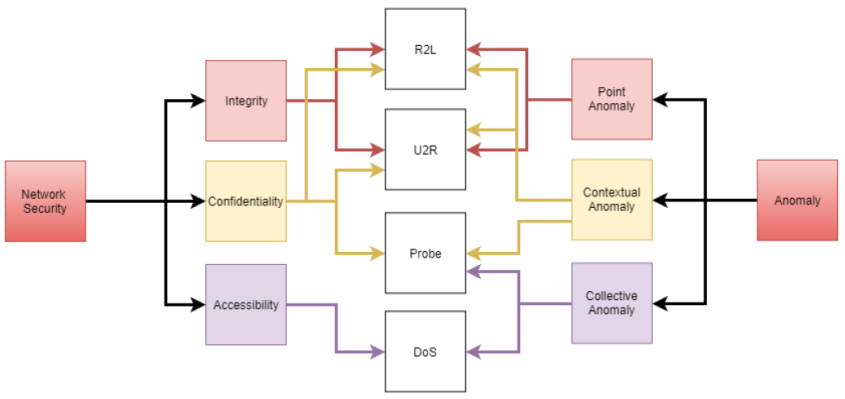
Hálózati támadások

A hálózati támadásokra többféle felosztás létezik. A tanulmányban az egyik fő csoportosítás használtuk fel, ami a következő:
- Túlterheléses támadás (DoS – Denial of Service)
  Az elfogadható válaszidő egy számítógépes alkalmazások esetén a legjobb esetben 0,1 szekundum. Az 1 szekundum válaszidő is még elfogadható a felhasználó számára. De ha 10 szekundum feletti a válaszidő, akkor a felhasználó figyelme máshova terelődik. [15]. Ebből az következik, hogy az internetes szolgáltatásokat nem minden esetben kell a lekapcsolásig terhelni, hanem elég csak annyira, hogy a felhasználók érdeklődése máshova irányuljon. A túlterheléses támadás egy olyan támadás, ami informatikai szolgáltatásokra irányul. A **túlterheléses támadás** álltalában nem veszélyesek, de ha több támadás jön több helyről (végpontról) az már gondod okozhat. Ha több helyről érkezik a támadás akkor azt **elosztott túlterheléses támadásnak** nevezzük. A következő típus a **reflektív támadás**, ami több végpontot használ, de nincs az ellenőrzésük felett. Csak a végpontokat felhasználva sokszorozza meg a forgalmat és irányítja a támadó felé. A fent említett támadásokkal a sávszéleséget, kapcsolatfelvételt vagy a forrásokat terhelik le. [16]
- Információ gyűjtés (Probe)
  Az információ gyűjtő támadás a célpont rendszeréről gyűjt információkat adatokat. Ezen a támadáson keresztül a támadó sok fontos információt tud beszerezni pl. a számítógépes hálózat felépítéséről, milyen operációs rendszert használnak. Ez a támadás nem okoz semmilyen sérülést az áldozatnak, evvel a támadással előkészítjük a következő támadást, ami már sérülést okozhat a rendszerre.
- U2E (Felhasználó a root felé)
  Ez a típusú támadásnál a támadó kísérletet tesz, hogy megszerezze a rendszergazda felhasználó fiókját annak érdekében, hogy fontos adatokat lopjon el. A támadó sérülékenységeket használhat ki vagy bruteforce támadást alkalmaz, hogy betudjon jutni a rendszergazda fiókjába.
- R2U/R2L (Távoli elérés a felhasználó felé vagy lokálisan)
  Ennél a típusú támadásnál a támadó beszivárog az áldozat hálózatába, és ott szerez jogosultságokat úgy, hogy hamis csomagokat küld a támandó számítógépre. Ebben az esetben is működik a sérülékenységek kihasználása vagy a bruteforece támadás. [17]

Anomáliák

Hogy ha egy adat kimagasló, szokatlan vagy az átlagtól eltérő akkor anomáliára lehet következtetni az adatkörben. A mi tanulmányunkban az anomáliák egy támadásra fog utalni, de lehet valami hiba is vagy akár átverés. Az anomáliát más néven is szokták hívni

outlire-nek. Az outlireek észlelése fontos mert nagy kárra is utalhat, amit fontos észlelni és javítani egy szervezetnek. Az outlireek detektálása három kategóriába lehet sorolni felügyelt tanulásra (supervised anomaly detection), felügyelt nélküli tanulásra (unsupervised anomaly detection) és ennek a kombinációjával (semi-supervised anomaly detection). A felügyelt tanulásnál az adatkörök tartalmaznak címkéket angolul lable az alapján határozza meg az anomáliákat. A felügyelt nélküli tanulásnál az adatbázis nem tartalmaz címkéket. Az a modell magától tanulja meg, hogy mi az anomália a minták segítségével.
Az outlireek három csoportját ismertetjük melyek a következők: pont-anomália, környezeti (kontextuális) anomália és együttes kollektív anomália. [17] [18]
„Pont-anomália alatt olyan objektumot értünk, amely önmagában is nagyban eltér a sokaság egészétől". Ami, azt jelenti, hogy ha drámaian eltér az adat a megszokottól akkor az pont-anomáliának nevezzük. Ha egy dolgozó csak délelőtt dolgozik és akkor jelentkezik be egy számítógépbe, de ha ugyan ez a dolgozó az esti órákban is bejelentkezik a számítógépbe azt már pont-anomáliának nevezzük. Ebben az esetben feltételezhetünk egy lehetséges támadást.
„Környezeti anomáliák közé tartoznak például olyan mérési eredmények, amelyek önmagukban véve nem szokatlanok, de az adott szituációban igen". Az anomáliákat kontextusában is kell figyelnünk mivel van olyan esett, hogy ha egy ember kisebb összegeket költ vásárlásra napi szinte, de ünnepekor nagyobb összeget költ ezt nevezzük anomáliának. Nem minden esetben feltételezzük, hogy támadás történt.
„Együttes anomáliák alatt olyan mérési eredményeket értünk, amelyek önmagukban nem tekinthetők anomáliának, együttesen viszont igen." Az együttes anomáliát könnyebb megérteni egy SYN elárasztási támadással. Ha két eszköz szeretne egymással kommunikálni TCP IP kapcsolattal akkor egy sémát kell követni. Ezt a sémát a SYN elárasztási támadással kilehet játszani. A kliens és a szerver között SYN, ACKSYN, ACK csomagot váltanak egymással és evvel a kapcsolat létre jön. A SYN elárasztásnál csak az első csomagot küldjük el, de nem egyszer, mint a sémában, hanem több ezerszer. Evvel a támadással a szervert képesek vagyunk leállítani vagy lelassítani, hogy ne legyen képes a rendeltetés szerű működésre. Szóval, ha csak egy SYN csomagot küldünk az még nem utal támadásra, de ha több ezret akkor azt együttes anomáliának tekintjük és egy támadást feltételezhetünk. [17]
A támadások és anomáliák között kapcsolat van, amit az 1. ábrán lehet látni.



1. ábra A hálózati támadások és anomáliák kapcsolata [17]

Kvantum számítógép

Az emberiség lassan, de biztosan felkészülhet a kvantum számítógépek korára. A kvantum számítógép ereje abban rejlik, hogy több állapotot vehet fel, ellentétben a mostani hagyományos számítógépekkel szemben. [19] A világ fel kell, hogy készüljön a kvantum utáni titkosításra is. [20]
A kvantum számítógéppel is lehetséges az anomáliák detektálása, kvantum anomália detektálásnak hívják. A gépi tanuláson alapuló anomália-észlelő algoritmusok széles választéka létezik, amelyek kiterjeszthetők a kvantum birodalomra. Ezek az új kvantum-algoritmusok nemcsak új kvantumjelenségek azonosításában, hanem biztonságos kvantumadatátvitelben, biztonságos kvantumszámításban és felhőn keresztüli ellenőrzésben is alkalmazhatók lehetnek. Ezek a kérdések még fontosabbá válhatnak, ahogy a felhőalapú kvantumszámítási rendszerek kvantuminternetté fejlődnek. [21]
A kvantumszámítás és a mélytanulás népszerű kutatás terület lett. A kvantumneruális hálózatokat (QNN) fejlesztik. Óriási lehetőség rejlik a két kutatási terület metszéspontjában. Ricks és Ventura volt az egyik legkorábbi, aki olyan QNN-t javasolt, amelyet kvantumáramkör-kapu segítségével modelleztek, amelynek súlyait kvantumkeresés és darabonkénti súlytanulás segítségével tanulták meg. [22]

ÖSSZEGZÉS

A számítógépes hálózatok védelme egy fontos terület. A mérnökök többféle védelmet építettek ki az idők során (tűzfal, vírusírtó, behatolás érzékelő rendszerek). Az új technológiák új védekezési lehetőségeket hoztak magukkal. A behatolás érzékelő rendszereket most már a gépi tanulási algoritmusokkal tovább fejlesztettük. Ezen belül a mélytanulási hálózatokat is alkalmazhatjuk. Ennek segítségével a behatolás érzékelés gyorsabb, pontosabb és a nulnapi támadások ellen is véd. A nem túl távoli jövőben pedig a kvantum számítógépek segítségével még gyorsabb behatolás érzékelő rendszerek megépítésére leszünk képesek. A kvantum számítógép és a mélytanulási hálózat napjainkban egy népszerű területé alakult ki.

FELHASZNÁLT IRODALOM

[1] Kritikus infrastruktúrák és kritikus infrastruktúrák (Letöltve: 2022.05.08)
[2] Internet growth statistics [Online]. Elérhető: https://www.internetworldstats.com/emarketing.htm (Letöltve: 2022.05.08)
[3] Internet usage statistics – The internet big picture [Online]. Elérhető: https://www.internetworldstats.com/stats.htm (Letöltve: 2022.05.08)
[4] Központi statisztikai hivatal – Internethasználók aránya [Online]. Elérhető: https://www.ksh.hu/stadat_files/ikt/hu/ikt0029.html (Letöltve: 2022.05.08)
[5] Statista – Number of internet of things connected devices worldwide from 2019 to 2030 [Online]. Elérhető: https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/ (Letöltve: 2022.05.08)
[6] ENISA threat landscape 2021 [Online]. Elérhető: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021/@@download/fullReport (Letöltve: 2022.05.08)
[7] Behatolás-érzékelők [Online]. Elérhető: http://old.sztaki.hu/~btoth/sztaki/IDS.pdf (Letöltve: 2022.05.08)

[8] Gépi tanulás a gyakorlatban [Online]. Elérhető: https://www.inf.u-szeged.hu/~rfarkas/ML21/index.html (Letöltve: 2022.05.11)
[9] Mély tanulás és gépi tanulás a Azure Machine Learning [Online]. Elérhető: https://docs.microsoft.com/hu-hu/azure/machine-learning/concept-deep-learning-vs-machine-learning (Letöltve: 2021.12.11)
[10] Emmanuel Tsukerman – Machine Learning for Cybersecurity [Online]. Elérhető: packpub.com (Letöltve: 2022.05.11)
[11] IDS 2018 [Online]. Elérhető: https://www.unb.ca/cic/datasets/ids-2018.html (Letöltve: 2022.05.11)
[12] Próbálgatásos technikák – nyers erő támadás [Online]. Elérhető: https://gyires.inf.unideb.hu/KMITT/c12/ch06s08.html (Letöltve: 2022.05.11)
[13] Cross site scripting (XSS)[Online]. Elérhető: https://www.cert.hu/cross-site-scripting-xss (Letöltve: 2022.05.11)
[14] Botnetek kialakulása, használatuk, trendjeik [Online]. Elérhető: http://hadmernok.hu/archivum/2008/2/2008_2_illesi.pdf (Letöltve: 2022.05.11)
[15] Response times 3 important limits [Online]. Elérhető: https://www.nngroup.com/articles/response-times-3-important-limits/ (Letöltve: 2022.05.11)
[16] Gyányi Sándor – Túlterheléses informatikai támadási módszerek és a velük szemben alkalmazható védelem [Online]. Elérhető: https://nke-repo.uninke.hu/xmlui/bitstream/handle/123456789/12255/ertekezes.pdf;jsessionid=CFF905A5AF971170147C040AD8536437?sequence=1 (Letöltve: 2022.05.11)
[17] Kahraman Kostas – Anomaly detection in networks using machine learning 2018.,[Online]. Elérhető: https://www.researchgate.net/publication/328512658_Anomaly_Detection_in_Networks_Using_Machine_Learning/link/5bd1d1bf458515343d58eddc/download (Letöltve: 2022.05.11)
[18] Bodon Ferenc, Buza Krisztián: Adatbányászat 2014., [Online]. Elérhető: https://regi.tankonyvtar.hu/hu/tartalom/tamop412A/20110064_55_adatbanyaszat/ar01s08.html (Letöltve: 2022.05.11)
[19] Beginner's guide to quantum machine learning [Online]. Elérhető: https://blog.paperspace.com/beginners-guide-to-quantum-machine-learning/ (Letöltve: 2022.05.11)
[20] ENISA – Post-quantum cryptography [Online]. Elérhető: https://www.enisa.europa.eu/publications/post-quantum-cryptography-current-state-and-quantum-mitigation/@@download/fullReport (Letöltve: 2022.05.11)
[21] Nana Liu, Patrick Rebentrost – Quantum machine learning for quantum anomaly detection [Online]. Elérhető: https://www.researchgate.net/profile/Nana-Liu-10/publication/320564334_Quantum_machine_learning_for_quantum_anomaly_detection/links/59ee00a84585154350e7fb85/Quantum-machine-learning-for-quantum-anomaly-detection.pdf (Letöltve: 2022.05.11)
[22] Siddhant Garg, Goutham Ramakrishnan – Advances in quantum deep learning: an overview [Online]. Elérhető: https://www.researchgate.net/publication/341311377_Advances_in_Quantum_Deep_Learning_An_Overview/fulltext/5eba1a614585152169c84087/Advances-in-Quantum-Deep-Learning-An-Overview.pdf (Letöltve: 2022.05.11)