

Alkalmazott mesterséges intelligencia felhasználási területei és biztonsági kérdései – Mesterséges intelligencia a gyakorlatban

Ekler Péter*, Pásztor Dániel

Budapesti Műszaki és Gazdaságtudományi Egyetem, Automatizálási és Alkalmazott Informatikai Tanszék, Budapest

Beérkezett: 2020. szeptember 22.; Elfogadva: 2020. október 22.

Összefoglalás

A mesterséges intelligencia az elmúlt években hatalmas fejlődésen ment keresztül, melynek köszönhetően ma már rengeteg különböző szakterületen megtalálható valamilyen formában, rengeteg kutatás szerves részévé vált. Ez leginkább az egyre inkább fejlődő tanulóalgoritmusoknak, illetve a Big Data környezetnek köszönhető, mely óriási mennyiségű tanítóadatot képes szolgáltatni.

A cikk célja, hogy összefoglalja a technológia jelenlegi állapotát. Ismertetésre kerül a mesterséges intelligencia történelme, az alkalmazási területek egy nagyobb része, melyek központi eleme a mesterséges intelligencia. Ezek mellett rámutat a mesterséges intelligencia különböző biztonsági réseire, illetve a kiberbiztonság területén való felhasználhatóságra. A cikk a jelenlegi mesterséges intelligencia alkalmazások egy szeletét mutatja be, melyek jól illusztrálják a széles felhasználási területet.

Kulcsszavak: mesterséges intelligencia, biztonsági kockázatok, kiberbiztonság, sérülékenység, neurális háló

The application areas and security concerns of artificial intelligence technology

Péter Ekler, Dániel Pásztor

Budapest University of Technology and Economics, Department of Automation and Applied Informatics, Budapest, Hungary

Summary

In the past years artificial intelligence has seen several improvements, which drove its usage to grow in various different areas and became the focus of many researches. This can be attributed to improvements made in the learning algorithms and Big Data techniques, which can provide tremendous amount of training.

The goal of this paper is to summarize the current state of artificial intelligence. We present its history, introduce the terminology used, and show technological areas using artificial intelligence as a core part of their applications. The paper also introduces the security concerns related to artificial intelligence solutions but also highlights how the technology can be used to enhance security in different applications. Finally, we present future opportunities and possible improvements. The paper shows some general artificial intelligence applications that demonstrate the wide range usage of the technology.

Many applications are built around artificial intelligence technologies and there are many services that a developer can use to achieve intelligent behavior. The foundation of different approaches is a well-designed learning algorithm, while the key to every learning algorithm is the quality of the data set that is used during the learning phase. There are applications that focus on image processing like face detection or other gesture detection to identify a person. Other solutions compare signatures while others are for object or plate number detection (for example the automatic parking system of an office building). Artificial intelligence and accurate data handling can be also used for anomaly detection in a real time system. For example, there are ongoing researches for anomaly detection at the

ZalaZone autonomous car test field based on the collected sensor data. There are also more general applications like user profiling and automatic content recommendation by using behavior analysis techniques.

However, the artificial intelligence technology also has security risks needed to be eliminated before applying an application publicly. One concern is the generation of fake contents. These must be detected with other algorithms that focus on small but noticeable differences. It is also essential to protect the data which is used by the learning algorithm and protect the logic flow of the solution. Network security can help to protect these applications.

Artificial intelligence can also help strengthen the security of a solution as it is able to detect network anomalies and signs of a security issue. Therefore, the technology is widely used in IT security to prevent different type of attacks.

As different BigData technologies, computational power, and storage capacity increase over time, there is space for improved artificial intelligence solution that can learn from large and real time data sets. The advancements in sensors can also help to give more precise data for different solutions. Finally, advanced natural language processing can help with communication between humans and computer based solutions.

Keywords: artificial intelligence, security risks, cybersecurity, vulnerability, neural networks

Bevezetés

Bár a mesterséges intelligencia területe az elmúlt években hatalmas fejlődésen ment keresztül, az alapjai már az előző évszázadra nyúlnak vissza. A Church–Turing tétel szerint egy számítógép képes bármilyen formális bizonyítás elvégzésére. Ezzel párhuzamosan az idegtudomány fejlődésével felismerték, hogy az emberi agy rengeteg kisméretű neuron, és az azok közötti kapcsolatokból áll, mellyel felmerült az elektronikus agy készítésének lehetősége.

A mesterséges intelligenciának nehéz pontos definíciót adni, mivel magát az intelligenciát sem könnyű pontosan körbeírni. Turing ennek meghatározása helyett egy tesztet vezetett be, melyben egy megfigyelő egy emberrel és egy géppel kommunikál írásban. Ha a megfigyelő a beszélgetés alapján nem tudja meghatározni, melyik fél az ember, és melyik a gép, akkor a gép mesterséges intelligenciával rendelkezik.

Az 1956–1974 közötti időszakokra sokan úgy tekintenek, mint a mesterséges intelligencia aranykorára: rengeteg támogatást kaptak kutatók ennek fejlesztésére, sokan optimistán álltak a jövőhöz. A szakasz végére viszont egyre több kritika érte a területet, mely mögött leginkább a korlátozott számítási kapacitás volt a felelős. A kritikák, illetve a jelentősebb eredmények elmaradása miatt a kormányzatok megvonták a támogatásokat, és beköszöntött az első „AI tél”. Ezt követte egy második fellendülés, egy második tél, majd egy jelentősebb időszak 1993–2011 között, amikor rengeteg ma is használt algoritmusnak alkották meg az elméleti hátterét.

A jelenlegi fejlődési szakasz 2011 óta tart, melyet elsősorban a Deep Learning, illetve Big Data technikák uralnak és amelynek az alapja a számítási kapacitás rohamos méretű fejlődése volt. Egyik oldalról elsősorban a videokártyák fejlődésének köszönhetően óriási párhuzamos számítási kapacitással rendelkezünk, mely nagyban elősegíti a jelenleg is használt neurális háló tanítását. Másik oldalról az internet, illetve az olcsó elektronika elterjedésével eddig még soha nem látott mennyiségű adat be-

gyűjtésére és feldolgozására vagyunk képesek, melyek elengedhetetlenek a betanításhoz.

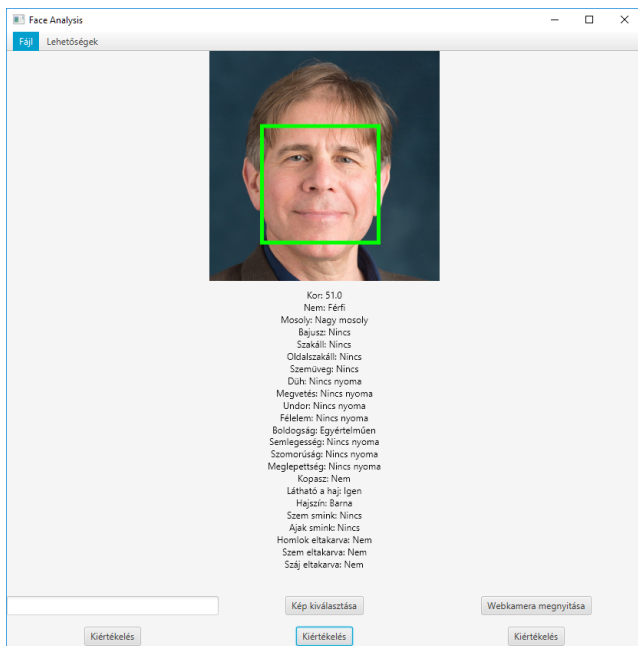
A cikk a továbbiakban az alábbi felépítést követi. A második fejezetben különféle felhasználási területeket mutatunk be a mesterséges intelligencia területén. A harmadik fejezetben a mesterséges intelligencia alkalmazásának kockázatával és biztonsági kérdéseivel foglalkozunk. A negyedik fejezet összegzi a tapasztalatokat és további irányokat vázol fel.

A mesterséges intelligencia felhasználási területei

A mesterséges intelligencia területén ma már rengeteg különböző algoritmus található, melyek számos szakterületen elegendő tanítóadat segítségével jobb eredményt érnek el a hagyományos megoldásokon felül.

Az elmúlt években óriási fejlődésen mentek keresztül a neurális hálókkal támogatott képfelismerő alkalmazások. Rendszeresen megrendezésre kerül az ImageNet verseny, melyen a versenyzők által készített programok a szervezők által megadott képeken próbálják beazonosítani a tárgyakat. 2012-ben ezt az AlexNet nevezetű neurális háló nyerte meg óriási fölényvel, 16.4%-os Top5 hibával (a neurális háló által legvalószínűbbnek talált öt tárgy egyike se helyes) (Alom et al. 2018). A jelenlegi legjobb megoldás a NoisyStudent (Xie et al. 2020), mely 98.7%-os Top5 hibát ér el, ezzel jobb eredményt elérve az emberek átlagos 95%-os hibájához képest.

A játékok világában is óriási változást hoztak a neurális háló. A DeepMind vállalkozás a kínai Go játékra tervezett számítógépes programot AlphaGo, illetve AlphaGo Zero néven. Míg az AlphaGo más világbajnokok játéka alapján tanult meg játszani, az AlphaGo Zero program csak és kizárólag saját maga ellen játszott (Silver–Schrittwieser–Simonyan 2017). Így tanítva a program képes volt mindösszesen három nap tanulás után 100–0 eredményre megverni az elődjét, mely maga is már képes volt a világbajnok Lee Sedol legyőzésére.

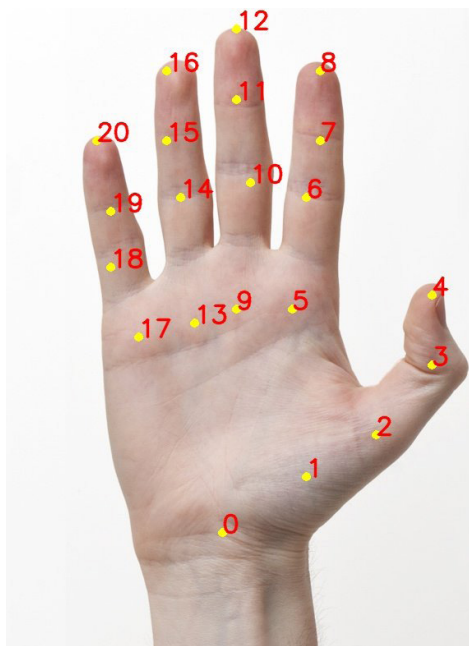


1. ábra | Arcfelismerő szoftver működés közben

Mesterséges intelligencia képfeldolgozási megoldások

A mesterséges intelligenciára számos alkalmazás épít, melyek már a mai világban is megtalálhatóak. Ezeknek futtatására sok esetben nincs is szükségünk nagyon erős számítógépre, gyakran elég akár egy laptop számítási kapacitása is.

Az arcfelismerés terén történt fejlődéseknek köszönhetően ma már rengeteg információ kinyerhető akár egy fénykép alapján. A Microsoft az Azure szolgáltatásán keresztül például elérhetővé tett egy arckereső -és felismerő szoftvert. Ez a képen lévő arcok megtalálása mellett képes az arc alapján életkort becsülni, nemet megállapítani, az arc különböző főbb pontjait megkeresni, de akár összetettebb dolgokat is vizsgálhatunk, mint például az

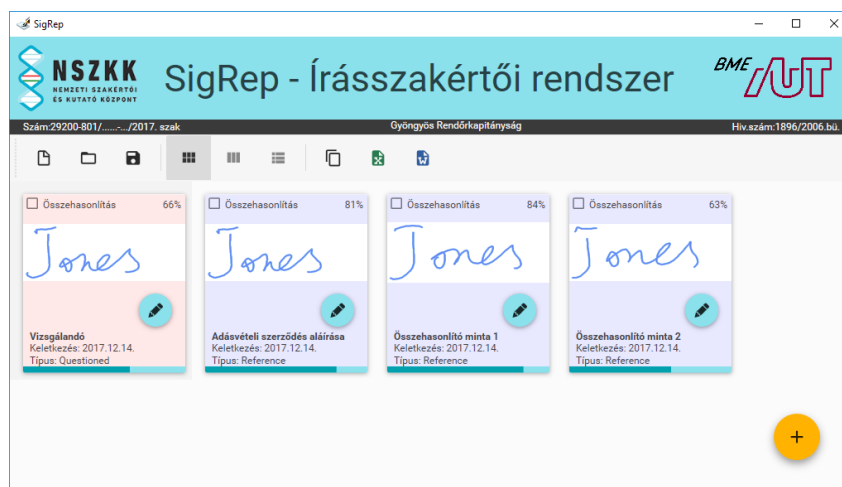


2. ábra | Kéz fő pontjainak felismerése

acról leolvasható gesztus, hajszín, szemszín, arcszörzet típusa, smink viselete. Az 1. ábrán egy prototípus formájában szemléltetjük az arcfelismerés adat lehetőségeket, mely az arcok összehasonlításán túl számos jellemzőt képes leolvasni, mint például az adott személy neve, életkora, kedve, hajviselete stb.

Az arc mellett képesek vagyunk a kéz gesztusainak detektálására is. A helyesen betanított program képes nagy pontossággal követni a kéz fő pontjait (2. ábra), mellyel így detektálhatjuk a kéz aktuális pozícióját, vagy akár egy mozgássort azonosíthatunk. Felhasználható például egy felhasználói felület irányítására, vagy akár a jelzés fordítására.

A kézi aláírások ellenőrzése és hitelesítése fontos terület elsősorban a pénzügyi, illetve a vállalati világban. A hamisított aláírások szűrésével könnyebben meg lehet



3. ábra | Aláírás-ellenőrző szoftver

akadályozni a személyazonossággal való visszaéléseket. A modern képfeldolgozásra optimalizált neurális hálók ebben a feladatban is segítséget tudnak nyújtani (Kóvári-Charaf 2013). A 3. ábrán látható alkalmazás például képes a felhasználó aláírása alapján javaslatot tenni az íránt, hogy valós vagy hamis az aláírás egy adott dokumentumon.

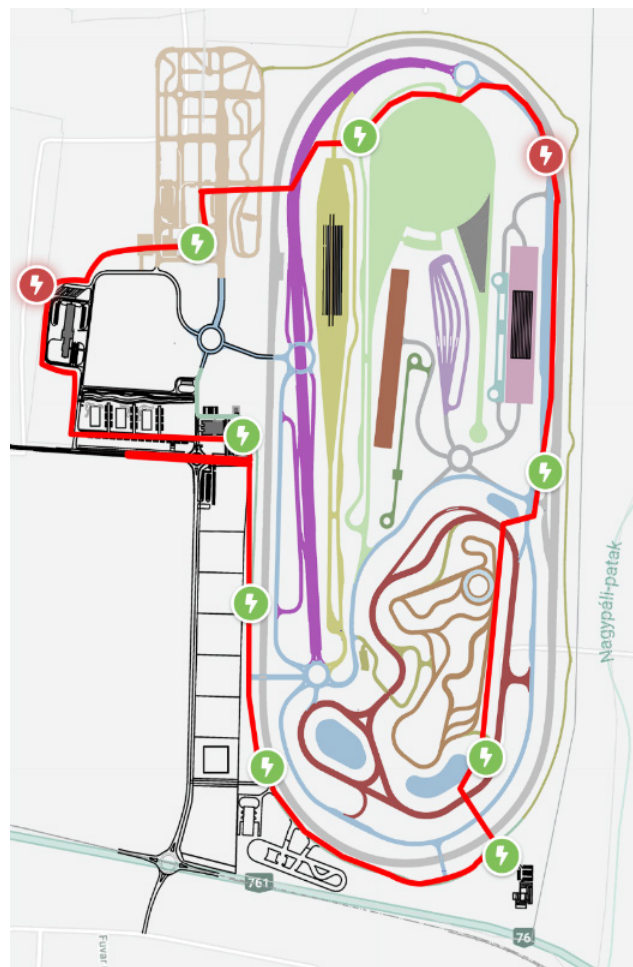
A fenti megoldások lehetővé teszik teljes és modern azonosítási funkciók megvalósítását akár video/kamerán keresztül alkalmazások számára is, mely jelentősen hozzájárulhat a digitalizációs fejlődéshez és az üzleti folyamatok hatékonyságának növeléséhez.

Az autók azonosításánál elterjedt módszer a rendszám-tábla beolvasása, hiszen ez a hatályos jogszabályok értelmében egyértelműen meghatározza az adott járművet. Ez egészen addig működőképes, ameddig nem cserélik ki a rendszám-táblákat az autókön ezeknek a rendszereknek a megkerülése érdekében. Ilyen helyzetben hasznos, ha a rendszám-táblák mellett az objektum más jellemzőit is vizsgáljuk, mint például kocsni típusa, színe, állapota (4. ábra).

Anomália detektálás tesztpálya környezetben

A tárterület dinamikus fejlődése és a felhőmegoldások segítségével manapság már nem probléma akár TB (TerraByte) méretű adatok gyors feldolgozása sem. Ilyen feldolgozás során szintén kiemelt szerep juthat a mesterséges intelligencia megoldások számára, amelyek akár közel valós időben is képesek különféle szolgáltatásokat nyújtani. Az egyik ilyen szolgáltatás lehet az anomália detekció, mely mielőbbi felfedezése komoly hatással lehet bármilyen informatikai megoldásban.

A Zalaegerszegen működő önvezető autó tesztpálya egy jó terep az anomália detekciós megoldások vizsgálatára. A pályán működik egy úgynevezett *Tracker* rendszer, melynek segítségével a pályára felhajtott járművek



5. ábra | A zalaegerszegi önvezető jármű tesztpálya Tracker megoldás az anomália detektáló modullal

folyamatosan nyomon követhetők valós időben. Ezen rendszer adatainak megfelelő gyűjtése alkalmas lehet arra, hogy egy mesterséges intelligencia megoldás megismerje a normál adatokat és eltérések esetén azonnal értesítést adjon a pálya kezelői számára. Ilyen eltérés lehet



4. ábra | Autóazonosítás másodlagos tulajdonságokkal együtt

egy autó sebességének jelentős változása, egy ütközés esetleges előre jelzése, vagy egy kanyar irreális sebességgel történő megközelítésének detektálása, de számos egyéb terület is megemlíthető, például kiugró energiafogyasztás, vagy jelentős kilengések a jármű adataiban (például fordulatszám). Az 5. ábra a *Tracker* rendszerbe épített energia monitorozó és anomália detektáló megoldás felületét szemlélteti.

Egyedi alkalmazások

A mesterséges intelligencia megoldások az ipari felhasználás mellett a hétköznapi használat során is számos előnnyel járnak. Prototípus jelleggel elkészült egy úgynevezett „Polgárőr” alkalmazás (6. ábra), melynél alapfunkció az általános információnyújtás, az aktuális hírek, változások bemutatása, értesítések (például KRESZ szabály változás) megjelenítése, helyfüggő információk nyújtása, interaktív szavazások és kvízek támogatása, bejelentési űrlapok kezelése. Egy ilyen megoldás azonban a napi használat során képes megismerni a felhasználókat, képes azonosítani azok szokásait és így lehetővé válik, hogy idővel a rendszer az adott felhasználó számára legfontosabb és legérdekesebb tartalmakat kiemelt helyen jelenítse meg, így biztosítva, hogy a fontos információk a releváns felhasználók számára biztosan eljuttanak.

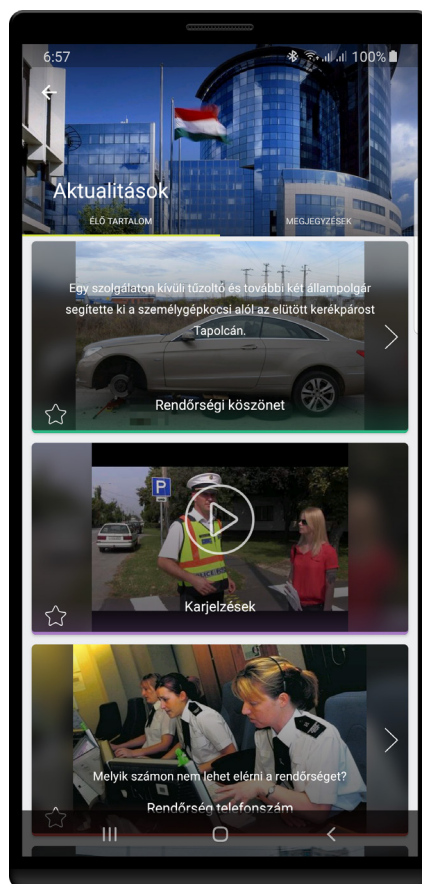
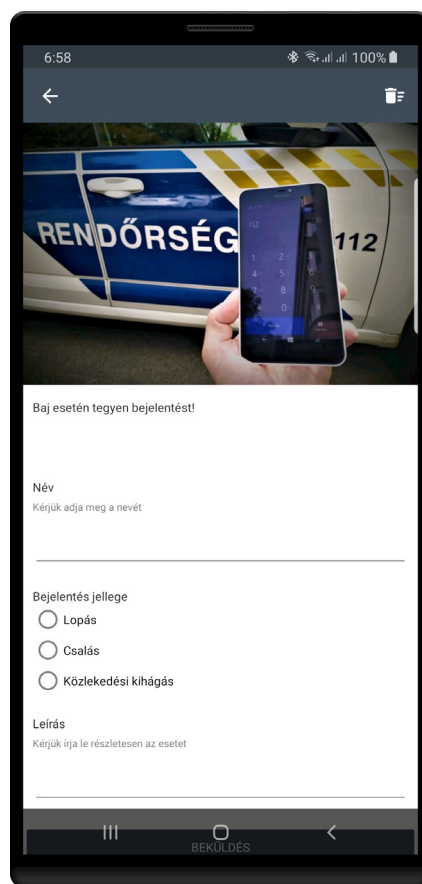
Az alkalmazott mesterséges intelligencia biztonsági kérdései

A mesterséges intelligencia alapú megoldások fokozatos terjedésével különösen fontos, hogy ezen megoldások biztonsági kérdéseit is megvizsgáljuk. Számos friss kutatás foglalkozik a mesterséges intelligencia biztonsága kérdéskörével. A *(Tadapaneni 2020)* cikk szerzői bemutatják, hogyan vezető vállalatok mesterséges intelligencia eszközöket alkalmaznak a szervezet működésében, azonban számos biztonsági kérdés felmerül az adatok kezelése során. A cikk ezen lehetőségeket vizsgálja, és bemutatja milyen fontos szerepe van a hálózati és egyéb biztonsági beállításoknak a mesterséges intelligencia alkalmazásakor.

A következőkben két aspektus szerint vizsgáljuk a mesterséges intelligencia biztonsági kérdéskörét. Egyrészt bemutatjuk milyen valós kockázatokat hordoz a technológia és annak alkalmazása, másrészt pedig ismertetjük, hogyan használható a mesterséges intelligencia a biztonság növelésére, mely egy új felhasználási terület a korábban felsoroltakon túl.

Kockázatok mesterséges intelligencia alkalmazásakor

Mesterséges intelligencia alapú megoldások nagy része valamilyen gépi tanulás eredményére épít. Gyakorlatilag elmondható, hogy a megoldás annyira intelligens amenny-



6. ábra | „Polgárőr” alkalmazás prototípus

nyire jó volt a tanulás folyamata és a tanításra használt adatok minősége. Például, ha egy hálózatot arcfelismerésre tanítunk akkor fontos, hogy minél színesebb legyen a tanító halmaz, minél szélesebb embercsoportot fedjenek le a mintaadatok, különben a rendszer elképzeltető, hogy jelentős hibákat fog véteni nem ismert csoportok esetén és egy hibás felismerés akár biztonsági kockázatokhoz is vezethet, ha például erre épül egy azonosító rendszer.

A tanításokhoz gyakran használt neurális hálók egyéb támadási felületekkel is rendelkeznek. Jiawei Su (2019) kutatásában mutatta be, hogy egy betanított képfelismerő hálónál sok esetben akár egy pixel megváltoztatása is elég ahhoz, hogy a predikció jelentősen megváltozzon, és másik címkével lássa el a képet (7. ábra). A támadó ezek mellett azt is befolyásolni tudja, hogy a melyik címkét adja vissza a háló az adott képre, így, ha ismeri a betanított háló paramétereit, könnyedén ki tudja játszani a rendszert.

Ahogy a cikkben is írják, az ilyen típusú változtatások elkerülhetőek a kép előfeldolgozásával, melyben detektálni és adott esetben el is lehet távolítani az ilyen típusú változtatásokat. Ez azonban nagyon teljesítményigényes, és növeli a késleltetését is az algoritmusnak, mely a valósidejű rendszereknél (mint például önvezető autók) jelenleg nem megengedhető.



Cup(16.48%)
Soup Bowl(16.74%)



Bassinet(16.59%)
Paper Towel(16.21%)



Teapot(24.99%)
Joystick(37.39%)



Hamster(35.79%)
Nipple(42.36%)

7. ábra

A címkézés befolyásolása egy pixelen keresztül (Su-Vargas-Konichi 2019).

A fekete az eredeti kép címkéje, a kék a megváltoztatott címke, míg a piros karikában látható a változtatás helye.

Egy komoly biztonsági kockázat napjainkban az úgynevezett *deepfake* alapú hamisítási technológia, amely mesterséges intelligencia és komoly számításkapacitás felhasználásával képes realiztikus audiovizuális tartalmakat előállítani, ahol a szereplő (például egy politikus) hitelesen kijelent valamit egy videon, azonban mind a kép, mind a szöveg mesterségesen lett előállítva korábbi anyagok alapján. Az ilyen megoldások számos esetben megteveszthetők lehetnek és fontos olyan megoldásokat kidolgozni, amelyek képesek ezeket a csalásokat azonosítani. Ilyen lehetőségről számolnak be a (Amerini 2019) cikk szerzői.

Összességében elmondható, hogy a mesterséges intelligencia és a hozzá kapcsolódó tanulási folyamatok és tanító adatok nagyon érzékeny és összetett rendszerek. Ezek védelme és a működés titkosítása kiemelten fontos. Ilyen rendszerek fejlesztésekor különféle hálózati és egyéb biztonsági megoldásokkal el kell kerülni, hogy a rendszer működése kívülről károsan befolyásolható legyen, illetve hogy akár a működésből vissza lehessen fejteni a tanító adathalmazt, vagy annak egy részét.

A biztonság fokozása mesterséges intelligencia segítségével

Természetesen ahogy sok más területen, a mesterséges intelligencia segítségével a kiberbiztonsági feladatok is hatékonyabbá tehetőek. Ebben a fejezetben pár területet mutatnánk be, melyben jelenleg vagy a jövőben előrelátólag óriási szerepet fognak kapni a gépi tanulással ellátott algoritmusok.

A mai modern, digitális világban óriási szerepet kap az információs rendszerek védelme, mivel azok számos érzékeny és értékes adatot tartalmazhatnak. Számos csoport létezik, melyek kifejezetten az online világban keresnek különböző rendszereken támadási felületeket, illetve végzik el a támadásokat.

Az első számú védelem, melyet a szoftverfejlesztők megtehetnek, a különböző fejlesztési és tervezési hibák elkerülése. Bár tökéletes programot senki se fog tudni készíteni, a nyelvhez tartozó ajánlások (best practices) betartásával jelentősen csökkenthető a hibák száma. Ezek mellett a legtöbb programozási nyelvhez készült statikus kódanalízis végző keretrendszer, mely képes a program fordítási idejében az ilyen ajánlások betartását ellenőrizni, illetve csak a programkód elemzésével hibákat keresni a programban.

Sajnos a statikus elemzési módszerek se tökéletesek. Szeretnénk, ha minél több hibát megtalálna, ez viszont jellemzően azzal jár, hogy rengeteg valójában nem hibás kódot is hibásnak jelöl (mivel az analízis végző rendszer nem feltétlen van tisztában minden kényszerrel, mint a programozó), melyek között így elvesznek a valóban is támadási felületet jelentő hibák. A statikus analízis további fejlesztésével tovább növelhető a pontosságuk, és ennek egyik módszere lehet a gépi tanulás alapú algoritmusok.

Ilyen elvek mellett fejlesztettek ki többek között például C és C++ nyelvhez mesterséges intelligenciát alkalmazó statikus analízátort (Russel et al. 2018). Ebben a kutatásban rengeteg már előre felcímkezett hibás kód mellé a kutatók még számos nyílt forráskódú projekten lefutott statikus analízátorok eredményeit használták az algoritmus tanítására. Az általuk tanított algoritmus egy neurális hálót használ, melyen belül kipróbáltak a tipikusan képek feldolgozására használt konvolúciós hálókat, illetve a beszélt nyelvek elemzését segítő visszacsatolt mély neurális hálókat.

Az így betanított rendszerüket tesztelve arra az eredményre jutottak, hogy mindegyik neurális háló jobb eredményt ér el az általuk tesztelt nyíltan elérhető keretrendszerekhez képest. A neurális hálókön belül is a konvolúciós háló jobb eredményt ért el a visszacsatolt hálóval szemben.

Az aktív kutatások mellett található hasonló rendszer a piacon. A DeepCode egy több nagyobb cég (mint például Google, Microsoft, Samsung) által használt szolgáltatás, mely a fejlesztői eszközökbe integrálódva képes intelligens hibakeresésre, illetve a hibák javítására szolgáló ajánlásokat tenni. A tanuló algoritmusnak köszönhetően képes a nyílt forráskódú projektekre feltöltött változtatásokat elemezni, azokból automatikusan javítani magát, így pontosabb és aktuálisabb hibajelentéseket képes adni.

A statikus kódelemzés csak az egyik módja a hibakeresésnek. A támadók azonban csak kivételes esetekben férnek hozzá az alkalmazás forráskódjához, így ez számukra nem jelent segítséget. Ilyen helyzetekben a támadó, illetve hibakereső tipikusan csak egy futás közbeni alkalmazáshoz fér hozzá a fejlesztők által létrehozott felületeken (például egy REST API) keresztül, ezeken kell olyan sérülékenységeket keresni, mellyel beljebb lehet kerülni a rendszerbe.

Ezen sérülékenységek megtalálásával rengeteg kutatás foglalkozik. Különböző adatbázisok vannak a hibák leírásáról, feltételeiről, kihasználási lehetőségükről. Azonban ezek ismerete és használata jelenleg a támadó személy feladata. Bár vannak eszközök, melyek a keresés bizonyos aspektusait képesek automatizálni, ezek hatékony használatához óriási tapasztalat és tudás szükséges.

Az ilyen irányú kutatások közül egyet emelnénk ki, melyben a szerző egy weboldalak sérülékenységét tesztelő általánosított rendszert hozott létre (Zech-Felderer-Breu 2017). Ebben egy tapasztalt kiberbiztonsági szakembernek definiálnia kell a különböző webes alapú támadási lehetőségeket egy általuk specifikált nyelvben. A rendszer ebből az információból képes új sérülékenységek létrehozására, illetve az így definiált adatbázis segítségével teszteket futtatni weboldalak ellen. Tesztjükben egy szándékosan hibakeresésre készített weboldalon futtatva nagy arányban találta meg a tipikus hibákat, a nehezebben kivitelezhető hibafelületek esetén viszont sokszor nem jelzett, vagy bizonytalan jelzést adott vissza. Ezt a rendszert kiegészítve egy tanuló algoritmussal ké-

pes lenne a rendszer további hibák keresésre, illetve a weboldalakon futtatott tesztek is célzottabbak lehetnének.

Összefoglalás, jövőbeli irányok

A cikkben bemutatásra kerültek a mesterséges intelligencia alkalmazási területei, melyeket több valós példán keresztül ismertettünk. Ezen felül kitértünk a mesterséges intelligencia biztonsági kérdéskörére is, megvizsgáltuk milyen veszélyeket és kockázatokat rejt a technológia használata és hogyan lehet a biztonság megerősítésére használni.

A technológia óriási mértékben fejlődik, számos megoldás várható a jövőben, melyek erősítik az ilyen megoldások terjedését. A Big Data megjelenésével, illetve a számítási kapacitás exponenciális növekedésével a tanuló algoritmusok továbbra is óriási fejlődési potenciállal rendelkeznek. Bár már most is rengeteg helyen használják, rengeteg kihasználatlan terület maradt még.

Az önvezető autók területén már most is használatban vannak a különböző mesterséges intelligenciát használó megoldások, azonban jelenleg még nem érték el a teljes autonómiát, egy vezetőnek mindenképp figyelnie kell az útra. A jelenlegi rendszerben két másodpercet adnak a vezetőnek a beavatkozáshoz, a jövőben ezt szeretnék kitolni tíz másodpercre, majd később a teljesen önálló vezetésre.

A nyelvek elemzésével, beszélgetni képes robotokban is hatalmas fejlődés lakozik még. Jelenleg képesek már helyes nyelvtannal beszélni, viszont tipikusan a szöveg környezetét, kontextusát nem tudják követni, hamar el-
lentmondásba keverednek magukkal. A jövőben a szövegértés további javulásával képesek lesznek akár emberek kiszolgálására is.

Köszönetnyilvánítás

A kutatás az NKFIH Magyarország (BME IE-MI-SC TKP2020) BME Mesterséges Intelligencia TKP2020 IE támogatásával készült. A kutatás FIEK_16-1-2016-0007 számú projekt a Nemzeti Kutatási Fejlesztési és Innovációs Alapból biztosított támogatással, a Felsőoktatási és Ipari Együttműködési Központ – Kutatási Infrastruktúra Fejlesztése (FIEK_16) pályázati program finanszírozásában valósult meg.

Irodalomjegyzék

- Alom, M., Taha, T., Yakopcic, C., Westberg, S., Sidike, P., Nasrin, M., Esecn, V. B., Awwal, A. & Asari, V. (2018) The history began from alexnet: A comprehensive survey on deep learning approaches. <https://arxiv.org/abs/1803.01164> [Letöltve: 2020.09.20]
- Amerini, I., Galteri, L., Caldelli, R. & Bimbo, D. A. (2019) Deepfake Video Detection through Optical Flow Based CNN. *IEEE/CVF International Conference on Computer Vision Workshop (ICCVW)*, Seoul, Korea (South), pp. 1205–1207
- Kóvári, B. & Charaf, H. (2013) A study on the consistency and significance of local features in off-line signature verification. *Pattern Recognition Letters*, Vol. 34, Issue 3, pp 247–255

- Russell, R., Kim, L., Hamilton, L., Lazovich, T., Harer, J., Ozdemir, O., Ellingwood, P. & McConley, M. (2018) „Automated Vulnerability Detection in Source Code Using Deep Representation Learning,” in IEEE, Orlando, FL, USA.
- Silver, D., Schrittwieser, J. & Simonyan, K. Mastering (2017) the game of Go without human knowledge. *Nature*, pp. 354–359
- Su, J., Vargas, D. V. & Kouichi, S. (2019) One pixel attack for fooling deep neural networks. *IEEE Transactions on Evolutionary Computation*, Vol. 23, Issue 5, pp. 828–841.
- Tadapaneni, N.-R. (2020) Artificial Intelligence Security and Its Countermeasures. *International Journal of Advanced Research in Computer Science & Technology*, Vol. 8, Issue 1
- Xie, Q., Luong, M. T., Hovy, E. & Le, Q. V. (2020) Self-training with Noisy Student improves ImageNet classification. <https://arxiv.org/abs/1911.04252> [Letöltve: 2020.09.20]
- Zech, P., Felderer, M & Breu, R. (2017) Knowledge-based security testing of web applications by logic programming. *International Journal on Software Tools for Technology Transfer* 21, pp. 221–246

A cikk a Creative Commons Attribution 4.0 International License (<https://creativecommons.org/licenses/by/4.0/>) feltételei szerint publikált Open Access közlemény, melynek szellemében a cikk bármilyen médiumban szabadon felhasználható, megosztható és újraközölhető, feltéve, hogy az eredeti szerző és a közlés helye, illetve a CC License linkje és az esetlegesen végrehajtott módosítások feltüntetésre kerülnek. (SID_1)