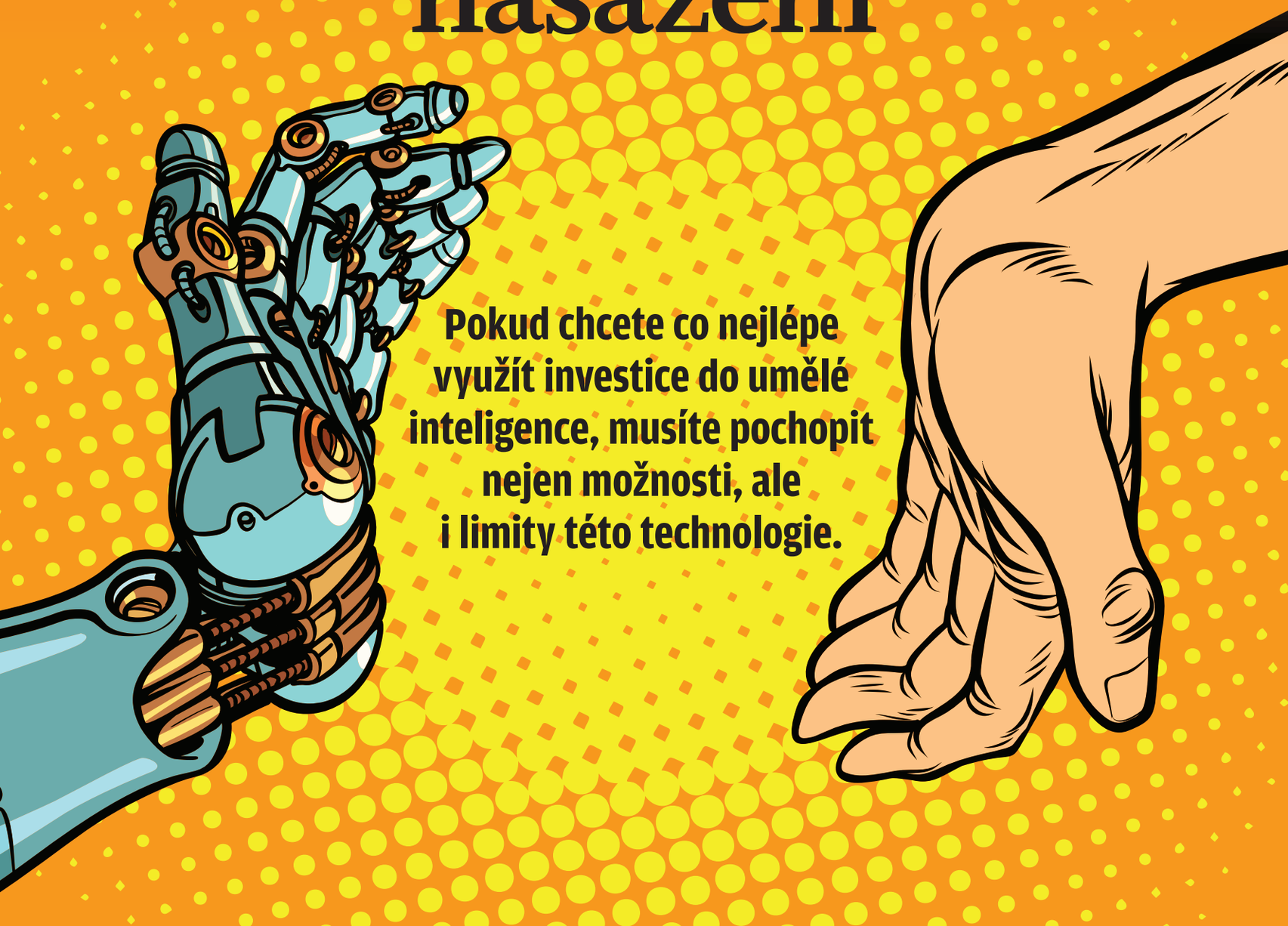
CIO BUSINESS WORLD COMPUTERWORLD

COMPUTERWORLD

ZVLÁŠTNÍ NEPRODEJNÁ PŘÍLOHA | ČERVENEC-SRPEN 2021

Umělá inteligence pro podnikové nasazení

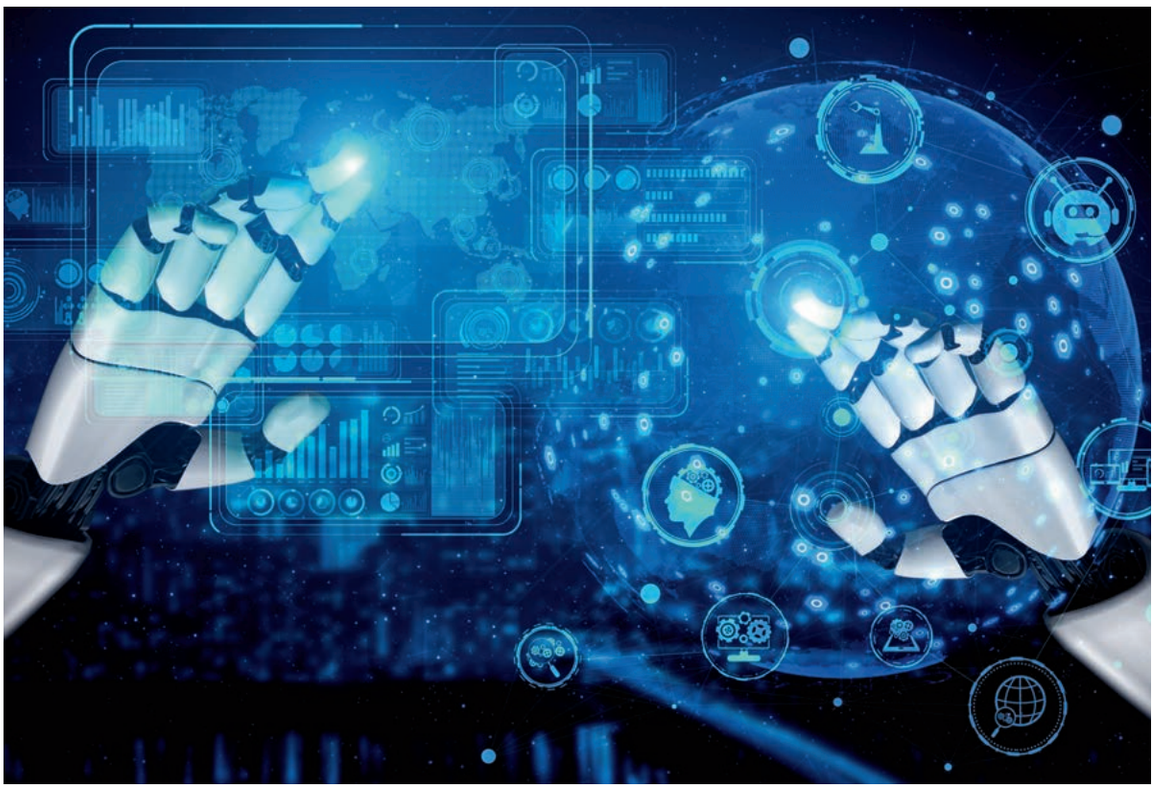


Pokud chcete co nejlépe využít investice do umělé inteligence, musíte pochopit nejen možnosti, ale i limity této technologie.

AI pomáhá v prostředí edge i IoT

MARIA KOROLOV

Použití umělé inteligence v okrajových prostředích může nejen snížit latenci a náklady na síťový provoz, ale také zlepšit bezpečnost a zpřístupnit sílu distribuované inteligence.



Spousta věcí v současné době nese nálepku „smart“ – počínaje žárovkami a konče auty. Jednotlivé funkce chytrých zařízení navíc zajišťuje některá podoba umělé inteligence či strojového učení.

Technologie AI už zdaleka nejsou vázané na velká centrální datová centra. Přesunem na okraj sítě (do prostředí edge) mohou podniky snížit latenci, zvýšit výkon, snížit požadavky na šířku pásma a umožnit zařízením fungovat i v okamžiku, když není k dispozici připojení k síti.

Jednou z hlavních příčin vhodnosti použití umělé inteligence v prostředí edge je, že se v terénu produkuje tak velké množství dat, že by tato data při svém přenosu ucpávala internet, pokud by je bylo nutné zpracovávat pomocí centralizovaných řešení cloud computingu či datových center.

„Nutnost posílat všechna tato data k centralizovanému zpracování do cloudu narazila na limity síťové šířky pásma a latence,“ vysvětluje Ki Lee, viceprezident společnosti Booz Allen Hamilton.

Vítejte tedy v éře edge computingu využívajícího AI.

Válka s boty

Jen opravdu málo firem zažívá tento problém v tak velkém rozsahu jako společnost Akamai. Ta totiž provozuje největší celosvětovou síť pro distribuci obsahu – podle posledního součtu zahrnuje přibližně 325 tisíc serverů ve více než 135 zemích. Každou sekundu tato síť zprostředkuje více než 100 terabitů webového provozu.

Kvůli množství dat produkovaných v terénu se při centrálním zpracování AI naráží na limity šířky pásma a latence přenosových cest.

Pro zlepšení výkonu a zabezpečení je klíčem edge computing, uvádí Ari Weil, tamější globální viceprezident pro produkty a oborový marketing.

Vezměme si například robotické systémy. *„Boty jsou na internetu obrovský problém,“* popisuje Weil. *„Útočí na zákazníky naší společnosti prostřednictvím automatizovaných útoků credential stuffing a DoS. Navíc ucpávají přenosové trasy neužitečným provozem, což nás stojí velké peníze.“*

Kyberzločinci používají boty také k pokusům o proniknutí přes obranu společností, výzkumných firem a zdravotnických organizací. Někdy jimi způsobované zlo nemá žádné hranice.

Hackeři například nedávno začali používat boty pro útoky na volná očkovací místa pro covid-19 ve stylu prodeje lístků.

Akamai nepřetržitě každou hodinu čelí 485 milionům žádostí od botů a 280 milionům pokusů botů o nejrůznější typy přihlášení.

V boji proti nim začala firma Akamai v roce 2018 zavádět systémy umělé inteligence v hraničním prostředí (edge) pro zjišťování, zda je konkrétní uživatel skutečným člověkem, nebo jestli je to robotická náhražka.

Následně používáme okamžité akce, jako například zvýšení zátěže, popisuje Weil.

„Například užíváme zátěž prostřednictvím JavaScriptu, který požádá jejich prohlížeč, aby udělal nějakou činnost. Pokud daný prohlížeč není skutečným prohlížečem, nemůže tuto práci vykonat. Snažíme se také vyvolat ‚bankrot‘ provozovatelů botů tím, že zvyšujeme výpočetní nároky, tak aby byl jejich provoz příliš drahý.“

V roce 2019 začala společnost Akamai používat také centralizované hluboké učení s cílem identifikovat chování botů a vyvinout lepší modely strojového učení. Tyto

modely jsou potom distribuované na okraj sítě (do prostředí edge), kde vykonávají svou práci.

Umělá inteligence se ve firmě Akamai využívá také pro analýzy hrozeb – threat intelligence. „*Je to problém z kategorie big dat,*“ popisuje Weil. „*Vezmeme obrovské množství údajů ve velkém datovém jezeře a zkoušíme pro ně použít různé modely, abychom našli škodlivé signatury. Jakmile vzory identifikujeme, můžeme je použít v celé platformě.*“

Někdy jsou zprávy neškodné, ale pocházejí ze škodlivého zdroje – například z řídicího centra.

„*Trénujeme edge model tak, aby rozpoznával provoz přicházející z konkrétního regionu či z konkrétní IP adresy, a aplikujeme zmírňující metody přímo na hranici sítě,*“ vysvětluje Weil.

Výsledkem je, že Akamai ušetří peníze, protože nemusí přenášet provoz generovaný boty či malwarem. Peníze ušetří i zákazníci, protože nemusejí platit za zbytečnou šířku pásma. Podniky také získají vyšší bezpečnost, protože musejí čelit menšímu počtu botů a malwaru.

Ve čtvrtém čtvrtletí roku 2020 dokázal systém firmy Akamai zablokovat 1,86 miliardy útoků na úrovni aplikací a zároveň zmařil více než 70 miliard útoků na přihlašovací údaje, konstatuje Weil.

Správa IoT

Umělá inteligence na okraji sítě může také snížit datové a síťové zatížení pocházející z technologií internetu věcí. Zařízení IoT mohou generovat obrovské množství informací, ale často jsou to údaje rutinní a opakující se.

„*Zařízení internetu věcí generují velké množství zpráv, že jsou v pořádku,*“ popisuje Weil. „*Je tedy potřeba v té záplavě informací najít signály ukazující na možné selhání. A to se následně musí dostat k příslušnému výrobci.*“

Využívá se k tomu technologie strojového učení nasazovaná do prostředí edge, která se naučí rozpoznávat kritické signály a daná data předem připraví k odeslání.

Vezměme si například propojené auto. Přesouvá se z jedné buňky do druhé, do jiných států, nebo dokonce do jiných nadmořských výšek a podnebí.

Odečtené údaje s hodnotami přiměřenými pro jedno místo však nemusejí mít přiměřené hodnoty pro místo jiné, nebo lze identifikovat problém tak, že se data mění příliš rychle. Pro přesnou analýzu těchto údajů je nezbytné využívat strojové učení.

„*Použití inteligence pro zařízení internetu věcí je v současné době jednou z oblastí největšího růstu IoT,*“ popisuje Carmen Fontana, členka IEEE a ředitelka pro cloud a nově vznikající technické postupy ve společnosti Centric Consulting.

Tento problém se podle ní vyskytuje v mnoha oborech, nejsou to jen automobily, ačkoli dopravní prostředky mají nejvyšší nároky na nízkou latenci.

„*Nechcete přenášet data do datového centra, abyste získali nějaké rozhodnutí, a výsledek poté přenášet zpět na cílové místo,*“ vysvětluje Fontana. „*Není na to čas.*“

Zpracování na okraji sítě je však výhodné i pro pomalu se pohybující či nehybná zařízení.

„*Dobrým příkladem mohou být solární panely umístěné někde mimo civilizaci,*“ popisuje. „*Nemají k dispozici dobré mobilní připojení ani síť Wi-Fi. Schopnost zpracovávat data a lokálně rozhodovat je skutečně důležitá.*“

Distribuovaná inteligence společnostem rovněž umožňuje snížit objem přenosů zpráv zpět ze zařízení, což snižuje náklady na síťové připojení a související spotřebu energie.

Velkou výzvou distribuované umělé inteligence je kybernetická bezpečnost – s velkým počtem chytrých edge zařízení se totiž významně zvětšuje i prostor pro případné útočníky.

„*Ukládání dat je poměrně drahé a není energeticky efektivní,*“ popisuje Fontana. „*Pokud tedy můžete nějak eliminovat velké množství dat, která byste jinak přenášeli a ukládali, potom je to skvělá metoda pro úsporu energie.*“

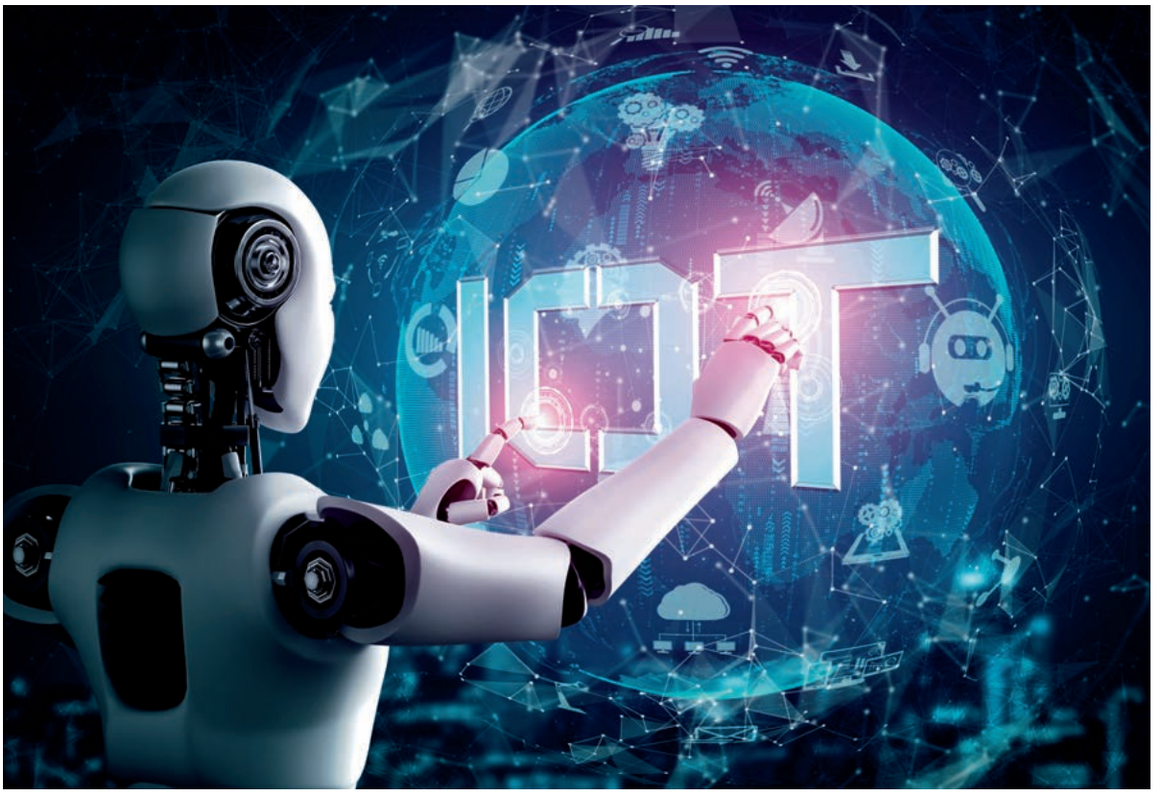
Umělá inteligence se také stále více používá v prostředí edge k tomu, aby zařízení získala další funkce.

„*Na zápěstí mám chytré hodinky a zařízení pro řízení zotavení organismu,*“ vysvětluje Fontana. „*To druhé jmenované zohledňuje mé vlastní hodnoty – srdeční tep a rytmus dýchání. Vypočítává, jak odpočaté mé tělo je a jak velká zátěž je pro mne vhodná pro další cvičení.*“

Decentralizované AI

Funkčnost umělé inteligence na okraji sítě může pomoci vytvořit inteligentní výpočetní prostředí distribuované do všech síťových zařízení – což je jedinečný přínos pro organizace, které vědí, jak toho využít.

Zejména obor služeb má velký zájem o distribuovanou inteligenci, říká Tim Driscoll, ředitel pro správu informací ve společnosti Itron, která se zaměřuje na tech- ▶



nologie pro správu energetických a vodních zdrojů.

„Měřiče na samotném okraji rozvodné sítě využívají aplikační platformu podobnou běžným chytrým telefonům,“ popisuje Driscoll. Tyto přístroje při své činnosti používají strojové učení pro reakce na různé stavy napětí a zatížení.

„Měřiče tak mohou nabízet příslušným operátorům poskytovatele služeb proaktivní doporučení v reálném čase pro řízení rozvodů.“

Ještě zajímavější však je, že tyto měřiče mohou spolupracovat a učit se ze svého vlastního chování v komunikační síti, z výkonu a spolehlivosti – následně si mezi sebou zvolí takzvaného vůdce, který mluví za síť a zastupuje je.

„To zjednodušuje správu sítě odstraněním potřeby centralizované analýzy,“ vysvětluje Driscoll.

Jak se rozvodné systémy vyvíjejí, aby zahrnovaly ještě více distribuované generování výkonu v rozvodné síti, začíná být edge computing pro tuto činnost nesmírně důležitý. Tradičně bylo pro elektrorozvodné sítě podstatné jen lokální zatížení – výroba a dodávka energie se řídily centrálně. Dnes jsou všechny tyto tři hodnoty proměnné.

„Je potřebné provozovat autonomní lokální řízení v reálném čase, zajištěné zpracováním v prostředí edge za využití strojového učení,“ popisuje Driscoll.

Kromě lepší latence a nižších nákladů přináší umístění systémů umělé inteligence a strojového

učení na okraj sítě také rychlejší fungování AI, uvádí Lee ze společnosti Booz Allen Hamilton.

Důvodem podle něj je, že decentralizovaná umělá inteligence v prostředí edge maximalizuje četnost kalibrace modelů, *„což nejen snižuje náklady na vývoj modelu, ale také to zvyšuje jeho výkon,“* vysvětluje.

Rizika a výzvy

Umělá inteligence v prostředí edge computingu však také představuje určitá rizika a výzvy, připomíná Lee. Patří do toho mimo jiné současný nedostatek standardů.

„Vidíme širokou řadu hardwarových zařízení pro edge computing, čipové sady procesorů, datové formáty a protokoly – a mnohé z nich jsou často navzájem nekompatibilní,“ uvádí Lee a dodává, že je potřeba se více zaměřit na vývoj společných otevřených architektur.

Nasazení AI v IoT dnes představuje výrazný růstový potenciál pro internet věcí.

Zaujal vás tento příspěvek? Čtěte související články s příbuznou tematikou on-line.

Kromě toho se mnoho hráčů v tomto prostoru zaměřuje na jednorázová řešení, která nejsou škálovatelná, chybí jim interoperabilita nebo jsou založená na tradičních modelech dodávky softwaru.

„Stále vidíme monolitické aplikace účelově vytvořené pro konkrétní zařízení,“ vysvětluje Lee. *„Z hlediska návrhu vídáme typické hvězdicové architektury, které ale selhávají, když dochází k omezení konektivity.“*

Další výzvou distribuované umělé inteligence je kybernetická bezpečnost. *„S velkým počtem zařízení nasazených v prostředí edge se zároveň významně zvětšuje útočný prostor,“* upozorňuje.

Experti už identifikovali útočníky využívající nezabezpečená zařízení internetu věcí – například botnet Mirai, který před pěti lety infikoval stovky tisíc koncových systémů. Jak stoupá počet řešení IoT a jak rostou jejich schopnosti, zvyšují se rovněž rizika, která tento stav představuje.

Jedním z přístupů je použít pro řešení problému strojové učení k detekci hrozeb. Hardware pro edge computing je obvykle méně výkonný a má různé limity, což omezuje možnosti zpracování dat, podotýká Lee.

Obrovský přínos v oblasti zabezpečení však může nastat při použití umělé inteligence v datových mikrocentrech v prostředích edge, uvádí Shamik Mishra, technologický ředitel pro konektivitu, výzkum a vývoj v konzultační společnosti Capgemini.

„Detekci hrozeb, správu zranitelností, zabezpečení perimetru a zabezpečení aplikací lze celkem dobře zajistit i v rámci prostředí edge,“ prohlašuje. Algoritmy AI mohou být decentralizované, aby detekovaly hrozby prostřednictvím detekce anomálií.

Objevují se také nové technologie, jako je Secure Access Service Edge (SASE), popisuje Mishra. Dochází tak ke kombinaci sítí WAN s funkcemi zabezpečení.

„Čím více různou funkcionalitu distribuujeme, tím více se systém stává zranitelným, protože roste prostor pro útoky na něj,“ připomíná. *„Aplikace pro edge computing tedy musejí pamatovat na zabezpečení již v rámci priorit samotného návrhu.“* ■

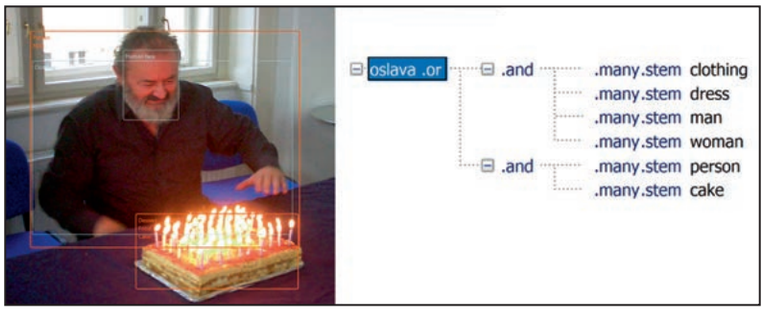
Umělou inteligenci je potřeba zapojit do rozhodovacích procesů přirozeným způsobem

MIROSLAV NEČAS

Když jsem se před více než patnácti lety setkal na univerzitě s umělou inteligencí, bylo to v předmětu ekonomicko-matematické metody.

Tehdy jsme neuronovou síť tvořili pomocí maker v Excelu. Technologie se od té doby hodně posunula a strojové učení je dnes jednou z běžně používaných metod zpracování dat. Pořád jde ale o metodu stochastickou. Hodí se všude tam, kde řešíme opakované slabě strukturované problémy a spíše než o optimální řešení jde o řešení dostatečné. V našich řešeních aplikujeme strojové učení na rozpoznání entit v textu, objektů v obrazu nebo převod mluveného slova do textu. To jsou úlohy, které nelze z kapacitních důvodů dělat ručně, a deterministické algoritmy se na ně nehodí.

Pokud extrahujeme entity z textu (abychom věděli, že se hovoří o určité osobě, firmě či místě), u entity typu e-mailu funguje deterministický algoritmus natolik spolehlivě, že strojové učení vůbec nemá smysl použít. Při extrakci entity typu telefonní číslo nebo osoba je stále deterministický algoritmus spolehlivější než strojové učení. Zejména díky tomu, že se můžeme opřít o znalost různých formátů telefonních čísel nebo znalost všech jmen a příjmení užívaných v ČR. Avšak u entit typu firmy či adresy již strojové učení dosahuje lepších výsledků. Je to tím, že jména firem mohou být obecná slova, rovněž je potřeba podle kontextu rozlišit mezi názvem organizace a jménem výrobku. S adresami je to podobné. Řada ulic a míst se jmenuje po významných osobnostech atd. Při detekci objektů v obraze či při převodu hlasu do textu jsou výsledky strojového učení dnes již zpravidla spolehlivější než výsledky deterministických algoritmů.



Výsledek vyhledávání „Oslava“ na základě definovaného dotazu

Při využití strojového učení je třeba stále mít na paměti několik věcí. Jde o stochastický algoritmus, proto je výsledek vždy do určité míry náhodný. Je daný kvalitou modelu a ta je daná kvalitou trénovacích dat. Jsou-li v trénovacích datech chyby, bude systém dávat chybné výsledky. Není-li trénovací množina dat úplná, systém si s některými problémy neporadí. Výsledek strojového učení je zkrátka konzistentní jen tehdy, když se zásadně neliší parametry provozních dat a parametry dat, na kterých byl systém natrénován. Změní-li se významně vstupní data, systém přestane dávat uspokojivé výsledky. Nepříjemné je, že u strojového učení automaticky nevíme, které parametry dat jsou pro určitý model významné.

Těchto omezení jsme si v Toveku dobře vědomi. Vyvinuli jsme proto vlastní postupy a nástroje pro přípravu trénovacích dat a ověřování natrénovaných modelů. To nám umožňuje zrychlit a zlevnit práci spojenou s manuálním značkováním dat, eliminovat chyby pramenící z lidské nepozornosti a zároveň rozpoznat, které parametry dat jsou pro určitý model významné. Například při tagování obrázku přímo definujeme oblast obrazu, jež je pro rozpoznání objektu určující. Jinak by se třeba mohlo stát, že se systém naučí identifikovat různé objekty podle doprovodného textu, nikoliv podle toho, jak vypadají.

Místo nahrazení lidí stroji se snažíme ulehčit jim od rutinních úloh a vytvořit prostor pro práci s vysokou přidanou hodnotou.

Využití umělé inteligence v našich řešeních umožňuje významné rozšíření různorodosti dat, která jsme schopní využívat pro vyhledávání informací, a rovněž významné rozšíření způsobu vyhledávání údajů. Příkladem je prohledávání fotek, které zachycují konkrétní situaci, např. oslavu. Tak jako v textu vyhledáváme informace podle struktury klíčových slov, ve fotkách vyhledáváme podle struktury rozpoznaných objektů, např. více než pět osob, láhev vína a dort. Tam, kde hledanou informaci nelze popsat, můžeme zase vytvořit model pro její rozpoznání, např. podpisová doložka v dokumentu nebo vyjádření názoru na určité téma. Tyto možnosti jsou velmi důležité pro využití obsahu stále rostoucího objemu fotek, videí a hlasových záznamů, pro vyšetřování incidentů či podvodů, různé kontroly a tvorbu znalostí o lokalitách, produktech nebo tématu.

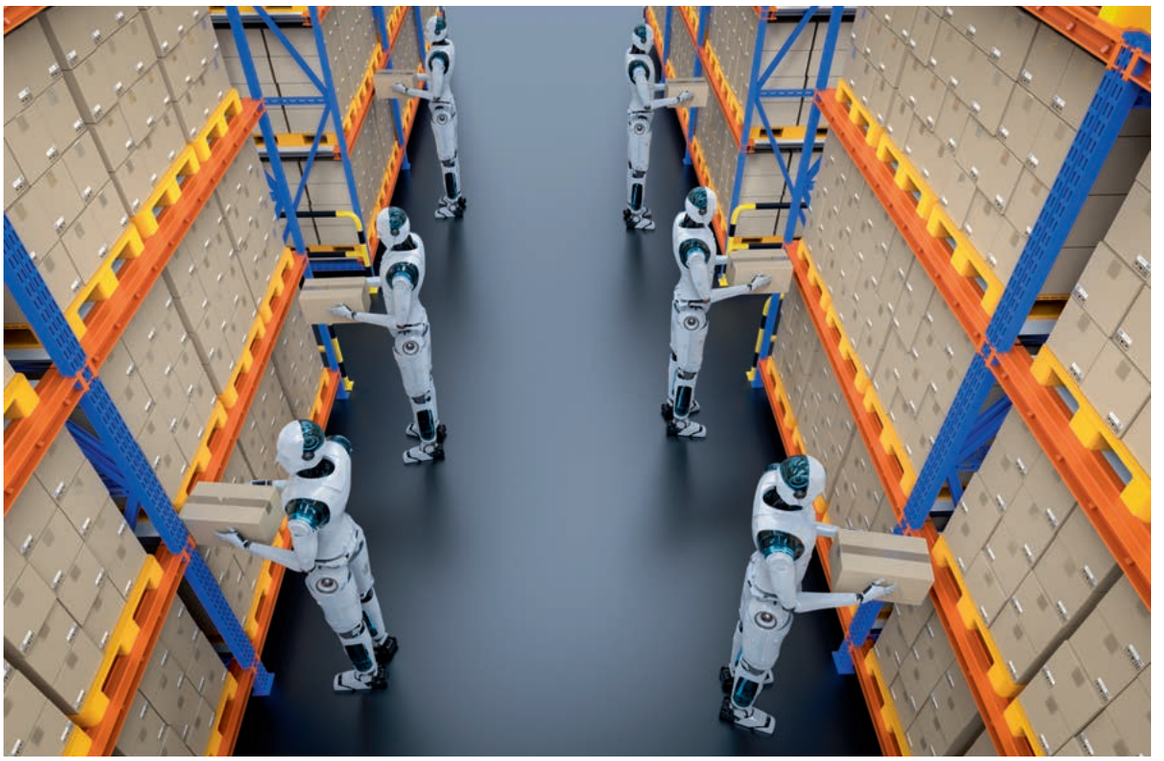
Samozřejmě existuje řada úloh, na které se umělá inteligence vyloženě nehodí. Kromě dobře strukturovaných problémů, na něž se více hodí deterministické algoritmy, jsou to i problémy, které se neopakují tak často, aby bylo na čem systém učit. Kapitolou samou pro sebe jsou situace, které vyžadují kreativní přístup a improvizaci. Na ty se žádný systém nehodí. Proto potřebujeme a budeme potřebovat stále více chytré a kreativní lidi. Místo toho, abychom usilovali o nahrazení šikovných lidí stroji, snažíme se ulehčit jim od rutinních a opakovaných úloh a poskytnout jim více času na práci s vysokou přidanou hodnotou. Proto kombinujeme strojové učení, deterministické algoritmy a vizualizaci informací, tak abychom do rozhodovacího procesu dokázali efektivně zapojit umělou inteligenci i lidský faktor. Věříme, že jedině s takovými nástroji budou naši klienti dlouhodobě konkurenceschopní. Budou pracovat efektivně a zároveň se dovedou adaptovat na měnící se podmínky na trhu.

Autor je business development manager, TOVEK.

Mýty, které brzdí zavádění AI

SANIYE ALAYBEYI

Pokud chcete co nejlépe využít investice do umělé inteligence (AI, Artificial Intelligence), je k tomu nutné pochopit nejen možnosti, ale i limity této technologie.



Metody umělé inteligence se dostávají stále hlouběji do pracovních prostředí. Nejenže nahrazují a zlepšují běžné činnosti, ale také rozšiřují či jinak mění ty zbývající. Pronikají do všech aspektů fungování firem a řídí organizační strategie.

Gartner ve své nedávné analýze předpovídá, že do roku 2025 bude AI nejdůležitější kategorií řídící rozhodování o podnikové infrastruktuře.

Přestože zájem o AI roste, řada mýtů o této technologii stále přetrvává. Ředitelé IT musejí tyto mýty rozpoznat a vyvrátit, aby mohli naplánovat zdravé strategie (nebo vylepšit současné) při řízení implementací projektů AI.

Díky pochopení fungování AI a souvisejících omezení mohou ředitelé IT lépe využít tuto technologii pro firemní potřeby.

Mýtus č. 1: AI je během krize covid-19 luxusem

Realita: Zájem a investice do AI nadále rostou i uprostřed covidové krize. Průzkum Gartneru zjistil, že od nástupu pandemie zvýšilo 24 % organizací investice do AI a 42 % jejich výši nezměnilo.

Během pandemie byla AI nejen důležitou pomocí při poskytování zdravotní péče pro odhady šíření viru a optimalizaci nouzových zdrojů, ale byla také významnou pomocí firmám všeho druhu při urychlení jejich snahy o obnovení provozu.

Umělá inteligence slouží během tohoto těžkého období jako důležitá pomoc pro optimalizace cen, zajištění kontinuálního provozu, podporu růstu příjmů a zlepšování interakcí se zákazníky.

AI lze použít k řešení široké řady firemních problémů, ale hodnotu přinese jen tehdy, když se pro ní použije vhodná strategie.

Přestože AI určitě není univerzálním všelékem, většina organizací si nemůže dovolit ignorovat její potenciál v boji proti bezprostředním i dlouhodobým vlivům pandemie.

Šéfové IT by proto měli aktivně propagovat AI nikoli jako luxus, ale jako mocnou technologii, kterou lze použít v pragmatických scénářích – k rychlejší analýze většího množství dat a k podpoře rozhodování, a to jak během pandemie, tak i po jejím skončení.

Mýtus č. 2: Nepotřebujeme strategii pro AI

Realita: AI lze použít k řešení široké řady firemních problémů, ale transformační hodnota začne vznikat jen tehdy, když se pro umělou inteligenci použije v podniku vhodná strategie.

IT může maximalizovat hodnotu AI spárováním firemních priorit s blízkými příležitostmi, zejména takovými, kde může výkon AI podpořit či rozšířit lidskou práci.

Začněte identifikací nejslibnějších případů použití umělé inteligence, které se hodí pro strategické iniciativy a kritické firemní funkce, jako je například automatizace administrativních činností, abyste získali více času na inovace.

Pravidelně revidujte přístup své organizace k AI a zajistěte, aby rozhodování o použití AI (nebo rozhodnutí o jejím nepoužití) bylo podložené předchozím výzkumem a rozvahou.

Mýtus č. 3: AI jen nahradí obyčejné a opakované činnosti

Realita: Postupem času mnoho technologií ovlivnilo způsoby lidské práce a rozsah potřebných dovedností. Některé profese tak zmizely, zatímco neustále vznikají nové.

V současné době je například vzácné narazit na pracovní pozici písařů s pracovní náplní psaní na

psacím stroji, na druhou stranu před deseti lety bylo vzácné se setkat s pozicí marketingového manažera pro sociální sítě.

Očekává se, že technologie AI budou mít významný dopad na způsob naší práce a učení i na to, jakou práci vykonáváme.

Umělá inteligence má potenciál nejen automatizovat úlohy považované za obyčejné či opakované, ale také pomoci zlepšit nebo změnit pracovní místa přetrvávající dosažením důležitějších úkolů.

AI například může přečíst tisíce právních smluv za pouhé minuty a získat z nich veškeré užitečné informace rychleji a s menším počtem chyb, než by to zvládli lidé s právním vzděláním.

Ředitelé IT mohou zjistit potenciální dopad umělé inteligence na současné úlohy nalezením činností, které by bylo možné rozšířit či zautomatizovat pomocí AI, jako je například řízení projektů a služby zákazníkům.

Personál lze poté přeškolit, aby se práce uskutečňovala s pomocí umělé inteligence s lepšími výsledky či rychleji. Je důležité často a transparentně komunikovat se zaměstnanci a zainteresovanými stranami, aby se podařilo rozptýlit obavy z použití AI a připravit týmy na přicházející změnu.

Mýtus č. 4:
AI a ML jsou totéž

Realita: AI je zastřešující termín pro širokou řadu počítačových metod. V rámci umělé inteligence existuje velká podoblast označovaná jako strojové učení (ML, Machine Learning), což je schopnost počítačů učit se bez výslovného naprogramování.

Technologii ML lze použít k rozpoznávání vzorů v rámci dat. Je obvykle dobrá pro řešení jedné konkrétní úlohy. ML lze například použít k rozhodování, zda daný e-mail je, či není spamem.

Podobně platí, že ML není totéž co hluboké učení (deep learning). Metody hlubokého učení a hluboké neurální sítě (DNN, Deep Neural Networks) jsou typem ML, který umožňuje úžasné výsledky.

To však neznamená, že je hluboké učení nejlepší technologií pro všechny problémy řešitelné pomocí umělé inteligence – neplatí tedy, že bude DNN vždy nejúspěšnější metodou AI pro konkrétní účel.

Ve skutečnosti se může mnoho současných problémů vhodných pro AI efektivně řešit pomocí systémů založených na pravidlech či s využitím tradičního ML.

Nejnovější špičkové možnosti umělé inteligence nejsou vždy nejefektivnějším řešením firemních potřeb. Povzbuzujte své datové vědce, aby vnímali technologie AI jako celek a používali takové metody, které se nejlépe hodí pro daný účel a cíl.

Pro komplexní problémy, zejména ty, které vyžadují více lidských poznatků, je často nejlepší kombinovat hluboké učení s dalšími metodami AI, jako jsou například fyzické modely a grafy.

Při rozhovorech se zainteresovanými stranami je důležité, aby došlo k vysvětlení těchto běžně zaměňovaných pojmů. Celou diskuzi o umělé inteligenci je dobré rozdělit do debat o jednotlivých metodách, jako je například ML, a demonstrovat, jak každá z nich dokáže řešit problémy reálného světa.

AI je zastřešující termín pro širokou řadu inteligentních počítačových metod.

Zaujal vás tento příspěvek? Čtěte související články s příbuznou tematikou on-line.

Mýtus č. 5:
AI se týká jen algoritmů a modelů

Realita: Návrh a použití algoritmů ML pro vytvoření prediktivního modelu je často nejjednodušší částí projektu AI. Náročnější fáze zahrnují zajištění, aby byl problém řešený pomocí umělé inteligence dobře specifikovaný, aby se nasbírala a uspořádala vhodná data, a nakonec nejtěžší část projektu AI – samotné zavedení.

Odhaduje se, že až do roku 2023 bude minimálně 50 % lídrů IT zápasit s přesunem svých prediktivních projektů umělé inteligence z fáze ověření konceptu do fáze zralosti vhodné pro produkční nasazení.

Šéfové IT by se měli zaměřit prostřednictvím konzultací se zainteresovanými stranami na popis problému, který má AI vyřešit. Je potřebné dostatečně v předstihu výslovně organizovat a řídit lidi, procesy a nástroje nutné pro testování, zavedení a další provozní aktivity pro umělou inteligenci.

Mýtus č. 6:
Všechny černé skříňky AI musejí odpovídat regulačním předpisům

Realita: Černá skříňka umělé inteligence je systém AI, jehož vstupy a procesy jsou uživatelům skryté. Různé případy využití umělé inteligence podléhají rozličným úrovním požadavků na vysvětlitelnost, a to v závislosti na zákaznícovi a regulačních aspektech – soukromí, zabezpečení, algoritmické transparentnosti a digitální etice.

AI, která generuje poznatky pro interní použití, nemusí nutně splňovat aspekty vysvětlitelnosti.

Naopak umělá inteligence, která rozhoduje o lidech (například v souvislosti se vhodností pro půjčky či úvěry), vyžaduje vysvětlitelnost. AI, jež rozhoduje v „uzavřené smyčce“ s důležitými důsledky (například při použití pro autonomní řízení vozidel), podléhá vysokým nárokům na vysvětlitelnost z etických a právních důvodů.

Ředitelé IT musejí zajistit, aby použití umělé inteligence splňovalo kritéria etiky a právních předpisů. Je také nutné zabezpečit podporu pro týmy zajišťující testování a validaci, protože jimi shromažďovaná data ovlivní potřebu vysvětlitelnosti použitého nasazení AI. ■