

Jubilejní 20. ročník konference o správě sítí a služeb (CNSM) 2024 se uskutečnil v Praze

20.11.2024 - | CESNET

Výhody a úskalí umělé inteligence

Mnohé technologie už nejsou výhradní doménou IT oblasti, jak dokazuje globální rozmach velkých jazykových modelů (LLM). Ty mohou být prospěšné i široké veřejnosti, ale zároveň je podle znalců potřeba k nim přistupovat se zdravou rezervovaností. Odborníci totiž varují před různými úskaly, jako jsou například tzv. halucinace, kdy model konstruuje nepravdivá fakta, nebo nedostatečné logické uvažování.

Příkladem rizikového – možná až nebezpečného – použití LLM jsou případy, kdy může jít o život. Dr. Noura Limam z University of Waterloo v Kanadě během panelové diskuze prohlásila: *„Kdybych potřebovala poradit, jak někomu zachránit život, rozhodně bych nevěřila ChatGPT.“* Přesto se experti shodují, že jazykové modely představují úžasnou technologii s velkým potenciálem. Výborně se hodí například pro generování strojově čitelných výstupů nebo jako uživatelské rozhraní v rodném jazyce, jak diskutovali významní odborníci prof. Luciano Paschoal Gaspary, dr. Carol Fung, prof. Gabi Dreo Rodosek a Ing. Jiří Rott.

Přednášející i diskutující se zaměřili na řadu témat, jako je zlepšování vlastností strojového učení aplikovaného na různé oblasti, zejména na správu a bezpečnost sítí. A k jakým výsledkům dospěli? Prioritní cíle zahrnují především vysvětlitelnost modelů a tvorbu vysoce kvalitních datových sad. K datovým sadám se navíc váže palčivý problém proměnlivosti vlastností v čase, tzv. „datové drift“. Ty jsou v síťovém provozu považovány za vážnou překážku, která brání praktickému nasazení klasifikátorů a detektorů založených na strojovém učení. Vyřešení této výzkumné výzvy zůstává dlouhodobým úkolem pro české i zahraniční výzkumníky a výzkumnice.

Budoucnost správy sítí a propojení s AI

Řadu zajímavých možností využití umělé inteligence odhalil Dr. Sebastián García, řečník z laboratoře StratosphereIPS na ČVUT v Praze. Podle něj má AI již v současné době velký potenciál v oblasti bezpečnosti a aktivní obrany. Závěrečná diskuze panelistů se však zaměřila na otázku úrovně vyspělosti umělé inteligence a velkých jazykových modelů, kde se jistě dá v blízké budoucnosti čekat velký pokrok.

Podle prof. Gabi Dreo Rodosek z univerzity v Mnichově budeme muset v budoucích sítích založených na 6G čelit mnoha výzvám, na které je vhodné aplikovat technologie, jakou je právě umělá inteligence. Za důležité aspekty budoucích sítí lze považovat „zero trust“ (návrh zabezpečení infrastruktur a systémů založený na principu nedůvěry vůči okolním zařízením, kde je nezbytná dostatečná autentizace a ověřování) a „zero touch“ (minimální kontakt lidských operátorů nebo uživatelů s cílovými zařízeními při jejich správě a konfiguraci). Automatizace a samoopravné systémy, což může poskytovat právě vhodně navržená umělá inteligence, se stanou klíčovými pro vybudování celkově fungujících technologií. Společnost Cisco a její řečníci, kteří se konference zúčastnili, představili aktuální stav a budoucnost produktů využívajících umělou inteligenci. Prezentace Cisco kladla velký důraz na oba komplementární pohledy: „AI pro síť“ a „síť (infrastruktury) pro AI“.

Poděkování organizátorům za jubilejní CNSM2024 v Praze

Konference CNSM2024 se uskutečnila díky společnému úsilí týmu sdružení CESNET a Fakulty informačních technologií ČVUT. *„Je to velká čest a zároveň důkaz, že Česká republika se již etablovala ve vědecké komunitě, která řídí tuto každoroční konferenci. Jsem velmi hrdý na svůj tým, díky němuž jsme mohli tuto prestižní akci uspořádat, a postavit se tak vedle pořadatelských zemí předchozích ročníků. Obzvlášť bych chtěl poděkovat dr. Karlu Hynkovi, mému bývalému doktorandovi, který odvedl skvělou práci v rámci celé organizace,“* uvedl dr. Tomáš Čejka, vedoucí výzkumného týmu v CESNETu a spolupředseda místního organizačního výboru.

<https://www.cesnet.cz/novinky/jubilejní-20-ročník-konference-o-sprave-siti-a-sluzeb-cnsm-2024-se-uskutečnil-v-praze-250>