دوشنبه 29 مرداد 1397 - 07:11

پژوهشگران "ام.آی.تی" انجام دادند

توسعه هوش مصنوعی مبتنی بر "رایانش ابری"

پژوهشگران "ام.آی.تی" روش جدیدی را برای ترکیب دو تکنیک رمزگذاری جهت حفاظت از داده‌ها توسعه داده‌اند.

پژوهشگران "ام.آی.تی" روش جدیدی را برای ترکیب دو تکنیک رمزگذاری جهت حفاظت از داده‌ها توسعه داده‌اند.

به گزارش ایسنا و به نقل از انگجت، پژوهشگران "ام.آی.تی" به منظور حفاظت از داده‌های مورد استفاده در "شبکه‌های عصبی مصنوعی"(online neural networks) روش جدیدی را توسعه دادند.

شبکه‌های عصبی مصنوعی سیستم‌ها و روش‌های محاسباتی نوین برای یادگیری ماشینی، نمایش دانش و در انتها اعمال دانش به دست آمده در جهت بیش‌بینی پاسخ‌های خروجی از سامانه‌های پیچیده هستند.

استفاده از "رایانش ابری" عمومی در حال افزایش است. رایانش ابری مدل رایانشی بر پایه شبکه‌های رایانه‌ای مانند اینترنت است که الگویی تازه برای عرضه، مصرف و تحویل خدمات رایانشی با به‌کارگیری شبکه ارائه می‌کند. رایانش ابری از ترکیب دو کلمه رایانش و ابر ایجاد شده‌ است. ابر در اینجا استعاره از شبکه یا شبکه‌ای از شبکه‌های وسیع مانند اینترنت است که کاربر معمولی از پشت صحنه و آنچه در پی آن اتفاق می‌افتد اطلاع دقیقی ندارد(مانند داخل ابر). در نمودارهای شبکه‌های رایانه‌ای نیز از شکل ابر برای نشان دادن شبکه اینترنت استفاده می‌شود. دلیل تشبیه اینترنت به ابر در این است که اینترنت همچون ابر جزئیات فنی‌اش را از دید کاربران پنهان می‌سازد و لایه‌ای از انتزاع را بین این جزئیات فنی و کاربران به وجود می‌آورد.

غول‌های فناوری مانند آمازون، گوگل و مایکروسافت چند سال است که پلتفرم‌های هوش مصنوعی مبتنی بر رایانش ابری را راه اندازی کرده اند که قادر به انجام وظایف محاسباتی سنگین از طریق استفاده از "شبکه‌های عصبی پیچشی" (convolutional neural networks) است.

شبکه‌های عصبی پیچشی رده‌ای از شبکه‌های عصبی عمیق هستند که معمولا برای انجام تحلیل‌های تصویری یا گفتاری در یادگیری ماشین استفاده می‌شوند. یک شبکه عصبی پیچشی از یک لایه ورودی، یک لایه خروجی و تعدادی لایه پنهان تشکیل شده‌ است. لایه‌های پنهان یا پیچشی هستند، یا تجمعی یا کامل.

سیستم امنیتی جدید که توسط پژوهشگران ام.آی.تی توسعه داده شده، شامل ترکیبی از دو تکنیک "رمزنگاری هم‌ریختی"(homomorphic encryption) و "مدارهای گسسته"(garbled circuits) است و به گونه‌ای طراحی شده که بسیار سریع‌تر از دیگر پلتفرم‌ها عمل می‌کند.

رمزنگاری هم‌ریختی نوعی از رمزنگاری است که به وسیله آن می‌توان بر روی متن رمز، عملیات خاص ریاضی انجام داد و عملیات ریاضی انجام شده عینا بر روی متن آشکار پیاده می‌شود.

"چیراگ جووکار"(Chiraag Juvekar) دانشجوی دکتری در رشته مهندسی برق و علوم کامپیوتری و نویسنده ارشد این مطالعه گفت: ما در این سیستم تنها از تکنیک‌هایی که کارآمدتر هستند، استفاده کرده‌ایم.

پژوهشگران سیستم هوشمند مذکور را "GAZELLE" را نامگذاری کرده و آنها را بهترین سیستم برای محافظت از داده‌ها مورد استفاده در شبکه‌های عصبی مصنوعی می‌نامند.

این سیستم به طور موثر از داده‌های آپلود شده محافظت کرده و پارامترهای شبکه را به درستی همانند دیگر سیستم‌ها انجام می‌دهد. با این حال GAZELLE ۲۰ تا ۳۰ برابر سریع‌تر از مدل‌های دیگر است.

این سیستم هوشمند بسیار هیجان انگیز است و ممکن است در آینده مهم‌ترین نقش آن در زمینه پزشکی باشد زیرا با استفاده از GAZELE، بیمارستان‌ها می‌توانند به طور ایمن و کارآمد نتایج خود را توسط رایانش ابری با سایر موسسات پزشکی همانند موسسات مراقبت سلامت به اشتراک بگذارند.