OUCH! 2023 - 05

SANS SECURITY AWARENESS

Mākslīgais intelekts: Kas par to jāzina?

Kas tas ir un kāpēc man tas būtu svarīgs?

Mākslīgais intelekts (MI) apraksta sistēmas, kas programmētas domāt un reaģēt tāpat kā cilvēki. Patiesībā mēs uzdevām tieši šos jautājumus MI risinājumam ChatGPT un saņēmām šādu atbildi.

Kas ir mākslīgais intelekts?

Mākslīgais intelekts (MI) ir cilvēka intelekta simulācija mašīnās, kas ir ieprogrammētas domāt un mācīties kā cilvēki. Tas ietver algoritmu un datorprogrammu izstrādi, kas spēj veikt uzdevumus, kuru īstenošanai parasti ir nepieciešams cilvēka intelekts, piemēram, atpazīt runu, saprast dabisko valodu, pieņemt lēmumus un spēlēt spēles. Ir vairāki MI veidi, tostarp uz noteikumiem balstīts MI, ekspertu sistēmas un mašīnmācīšanās.

MI ir tik spēcīgs tāpēc, ka tas spēj simulēt cilvēka saprātīgumu un spriešanas spējas, taču tam iespējams analizēt eksponenciāli daudz vairāk informācijas nekā jebkuram cilvēkam un darīt to ievērojami ātrāk.

MI koncepcija nav jauna. MI, kas sākotnēji aprakstīts zinātniskās fantastikas romānos, tiek attīstīts jau vairākus gadu desmitus. Iemesls, kādēļ tagad par to tik daudz dzirdat, ir tas, ka pirmo reizi ikvienam ir iespēja mijiedarboties ar MI un redzēt tā patieso funkcionalitāti.

Tiešsaistē pieejamais MI tērzēšanas robots ChatGPT ir viens no pirmajiem publiski pieejamajiem risinājumiem, kas spēj atbildēt kā īsts cilvēks, izturot tā dēvēto Tjūringa testu. Šajā testā tiek noteikta mašīnas spēja demonstrēt saprātīgu uzvedību, reālam cilvēkam mijiedarbojoties ar mašīnu, izmantojot teksta tērzēšanas kanālu. Ja cilvēks nespēj noteikt, vai viņš mijiedarbojas ar mašīnu vai cilvēku, tiek uzskatīts, ka mašīna ir izturējusi testu. MI risinājumi mūsdienās ir pirmie publiski pieejamie, kas spēj testu izturēt.

Tomēr tiešsaistes sarunas ir tikai sākums tam, ko spēj paveikt MI. Tagad ir pieejami mākslīgā intelekta risinājumi, ar kuriem var izveidot videoierakstu par personu, kas māca skolēnus jebkurā valodā, analizēt veselības kartes un ātri noteikt, kam, visticamāk, ir vēzis, kā arī izveidot ziņu rakstus vai esejas par jūsu izvēlētu tēmu, ģenerēt attēlus bērnu grāmatām vai izveidot kodu jaunām datorprogrammām. Lai gan MI ne vienmēr ir kaut kas tāds, no kā būtu jābaidās, tomēr pastāv daži ar to saistīti riski, par kuriem ir jāzina.

Mākslīgā intelekta riski

1. **Cilvēka atveide**: MI risinājumi var ierakstīt personas balsi — jūsu balsi — un pēc tam to izmantot, lai reāllaikā atskaņotu audio, kas skan tieši tāpat kā jūs, sakot visu, ko vēlas, lai jūs atdarinātu. Tātad kiberuzbrucējs var ierakstīt balss ziņu, kas izklausās pēc jums, maldinot jūsu kolēģus, bankas darbiniekus vai ģimenes locekļus un liekot domāt, ka esat zvanījis un lūdzis viņiem veikt kādu darbību. MI to var izdarīt arī ar attēliem vai video. Dažkārt šo tehnoloģiju dēvē par "dziļviltojumiem", jo MI risinājums var izmantot esošo jūsu attēlu vai videoklipu un ar tā palīdzību radīt pilnīgi jaunus attēlus vai videoklipus (tostarp jūsu balsi), kuros redzamas jūsu darbības, ko jūs nekad neesat darījis.

2. **Nepareizas atbildes**: Dati vai atbildes, ko nodrošina MI, var būt nepareizas. MI bieži izmanto publiski pieejamu informāciju no interneta, un tā atbildes var ietekmēt tā izstrādātāju aizspriedumi. Kamēr tipiskās meklētājprogrammas ir izstrādātas tā, lai sniegtu jums "labāko" vai pareizāko atbildi uz jūsu vaicājumu, tādi risinājumi kā MI var būt izstrādāti tā, lai sniegtu jums cilvēciskāko atbildi. Tas, kura atbilde ir labāka, ir atkarīgs no tā, ko cenšaties sasniegt.

3. **MI nevienlīdzība**: MI kļūstot par jaunāko aktuālo tehnoloģiju, šobrīd ir burtiski simtiem jaunuzņēmumu, kas piedāvā dažādus MI pakalpojumus. Daudzi no tiem vēlas saņemt jūsu informāciju vai kredītkarti, lai veiktu izmēģinājumu. Esiet uzmanīgi — ne visi MI pakalpojumi ir uzticami. Pirms reģistrējaties un izmantojat MI pakalpojumu, veiciet izpēti.

4. **Jūsu konfidencialitāte:** Katru reizi, kad izmantojat mākslīgā intelekta sistēmu vai mijiedarbojaties ar to, piemēram, tērzējot tiešsaistē ar ChatGPT, ņemiet vērā, ka jebkuru sistēmā ievadīto informāciju tā var ne tikai apstrādāt, bet arī saglabāt un izmantot, lai sniegtu atbildes citiem. Tas nozīmē, ka, ievadot jebkādu personisku informāciju par sevi vai konfidenciālu darba informāciju, šī informācija tiks saglabāta un, iespējams, kopīgota vai pārdota citiem. Nedalieties un neievadiet darbā nekādu informāciju, ko uzskatāt par sensitīvu, personisku vai konfidenciālu.

Mākslīgā intelekta (MI) nākotne

Mākslīgais intelekts joprojām ir ļoti agrīnā attīstības stadijā, līdzīgi kā pirms divdesmit līdz trīsdesmit gadiem bija internets. Lai gan mēs varam sagaidīt strauju MI attīstību un ieviešanu, ir ļoti grūti prognozēt, kāda būs tā ietekme. Vienkārši apzinieties, ka šīs iespējas ir pieejamas, un, izmantojot MI, esiet ļoti piesardzīgi, kādu informāciju ievadāt un kopīgojat.

Resursi

ChatGPT: https://chat.openai.com/chat
Tjūringa tests: https://en.wikipedia.org/wiki/Turing_test

Tulkojums: CERT.LV