precognox

Jóföldi Endre

“AI Snake Oil” - “MI csodaszer”

Irreális igéretek és túlzó elvárások, biztonsági kérdések

2025. szeptember

Az intelligencia... Az absztrakcióra, logikára, megértésre, öntudatra, tanulásra, érzelmi ismeretekre, érvelésre, tervezésre, kreativitásra, kritikus gondolkodásra és problémamegoldásra való képesség.

50X több adat

Látás, nagy sávszélesség
4 ÉVES GYEREK,
$1x10^{15}$ bytes

Szöveg, alacsony sávszélesség
LLM, $2x10^{13}$ bytes

YANN LECUN
VP & Chief AI Scientist at Meta

Post | Feed | LinkedIn

MIT SLOAN
CIO SYMPOSIUM

AI
BABSON COLLEGE
Foundations
of AI

precognox

"Using LLMs for simple tasks is sometimes like using a bazooka to go after mosquitoes.

Do your research first, and then choose your tools wisely."

KATHARINE CLARKE
March 2025, Boston
LinkedIn

"Garbage is garbage out was true for regular IT solutions, garbage In is garbage out **amplified** is the reality for AI systems"

AI projects are data projects indeed.

GARY ARORA
Deloitte AI&Cloud leader, Healthcare
LinkedIn

Managing data in the Age of Data-Driven AI:
New challenges and opportunities

Before GenAI:

Structured Data Was Our Comfort Zone

Post-ChatGPT:

Unstructured Data is Now Strategic

precognox

IVAN LEE
Datasaur, CEO

"Only 1% of enterprise data has so far been accessed by generative AI (genAI) models"

Arvind Krishna
CEO at IBM

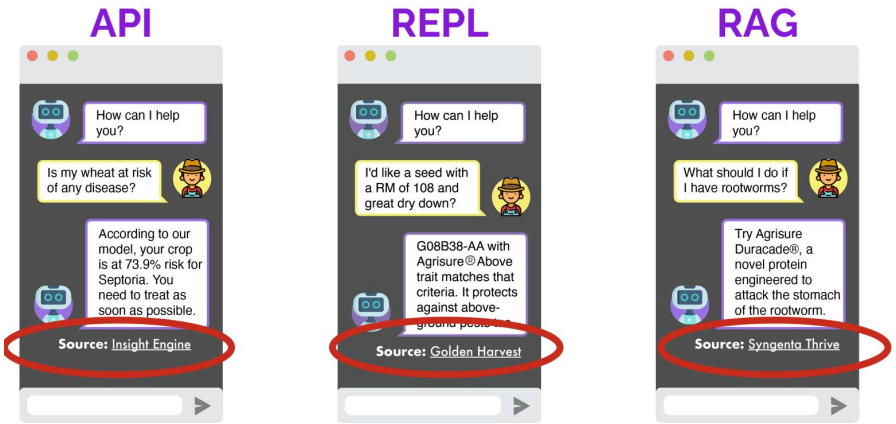
You need a number of fine tuned smaller models at your organization.

Building Trustworthy AI Agents:
Lessons from Digital Agriculture

SERG MASIS
Syngenta, Principal AI Scientist

Team - 8 people
Length - 6 months
Size - 50 MM

~ 100M HUF



precognox

Problems with generative AI?

HALLUCINATION

LLMs (Large Language Models) tend to "invent" or "hallucinate" information that does not reflect reality. This means that LLMs often make statements that seem confident but are not based on real data or sources. This can be especially problematic in applications where accuracy is crucial.

INPUT LENGTH ISSUES

Depending on parameterization, issues can arise where the LLM highlights only the extremes or only the beginning/end of the data set.

UNPREDICTABILITY

It will not run the same way twice. Even two consecutive identical questions may not yield the same answer.
A small prompt change → big difference.

BIAS

Any LLM reflects stereotypes built from the input data.

SECURITY ISSUES

Data sharing, legal risks, data protection, data leakage, adversarial prompting, template manipulation, hostile code within the LLM.

TECHNICAL CHALLENGES

Resilience, fault tolerance, scalability, load handling, infrastructural decisions, and optimization

A mesterséges intelligencia adatainak védelme: A 7 fázis

A KIHÍVÁS

A mesterséges intelligencia projektek 70–82%-át a Proof of Concept (POC) / Minimum Viable Product (MVP) szakaszban szüneteltetik vagy törlik a munkaerő felkészültségében és a mesterséges intelligencia adatbiztonságában tapasztalható hiányosságok miatt.

A megoldás
7 kulcsfontosságú fázis?

1.
Adatforrás biztonsága

2.
Adatinfrastruktúra biztonsága

3.
Átmenő adatok biztonsága

4.
API biztonság az alapmodellekhez

SOL RASHIDI
Cyera,
Chief Strategy Office, AI & Data

A megoldás: 7 kulcsfontosságú fázis?

5.
Alapmodell védelme

6.
Incidenskezelés MI alapú adatszivárgások esetén

7.
CI / CD a modellekhez (biztonsági horgokkal)

Fókuszáljon az adatokra, hogy túléljük az MVP-t!

SOL RASHIDI
Cyera,
Chief Strategy Office, AI & Data

MI a kiberbiztonságban: Kétélű fegyver

Nem csupán védelem, hanem fegyver is

1. Cyberbiztonság előbb rosszabb lesz, mielőtt jobb lehetne!

2. Kettős felhasználású MI itt van

3. Árnyék MI (Shadow AI) valódi kockázat

4. A védelemnek skálázódni kell a támadással

5. Stratégiába be kell kerülnie: kockázat

STUART MADNICK
MIT,
Professor of Engineering Systems

What kind of AI future are we building?

1.
Human-complementary AI
is the growth engine we're ignoring.

2.
Automation is easy;
transformation takes leadership.

3.
Be the next Ford, not the next chatbot.

DAREN ACEMOGLU
MIT professor,
2025 Nobel prize in economics

Hogyan készülhet egy cég az AI alkalmazására?

+ **AI tudatosság és oktatás**
  Döntéshozók és stakeholderek megismerkedése az AI alapú megoldások tárházával, lehetőségeivel, pros and cons
+ **Adatstratégia**
  (CDO / adatelőkészítés - tisztítás / strukturált és biztonságos adattárolás / flow of data stb)

  Gyűjtsétek össze a belső szöveges adatokat

  Nézzetek körül a szervezeten kívül is (Open source intelligence):
  Mi lehetne számunkra értékes?

+ **Infrastruktúra** - helyben, vagy felhőben, harmadik félre bízva
+ **Cybersecurity**

NAME SEARCH, KYC and AML solutions

Name matching

알 카포네	97,7 %
Аль Капоне	99 %
アルカポネ	99 %

Al Capone

Watchlists

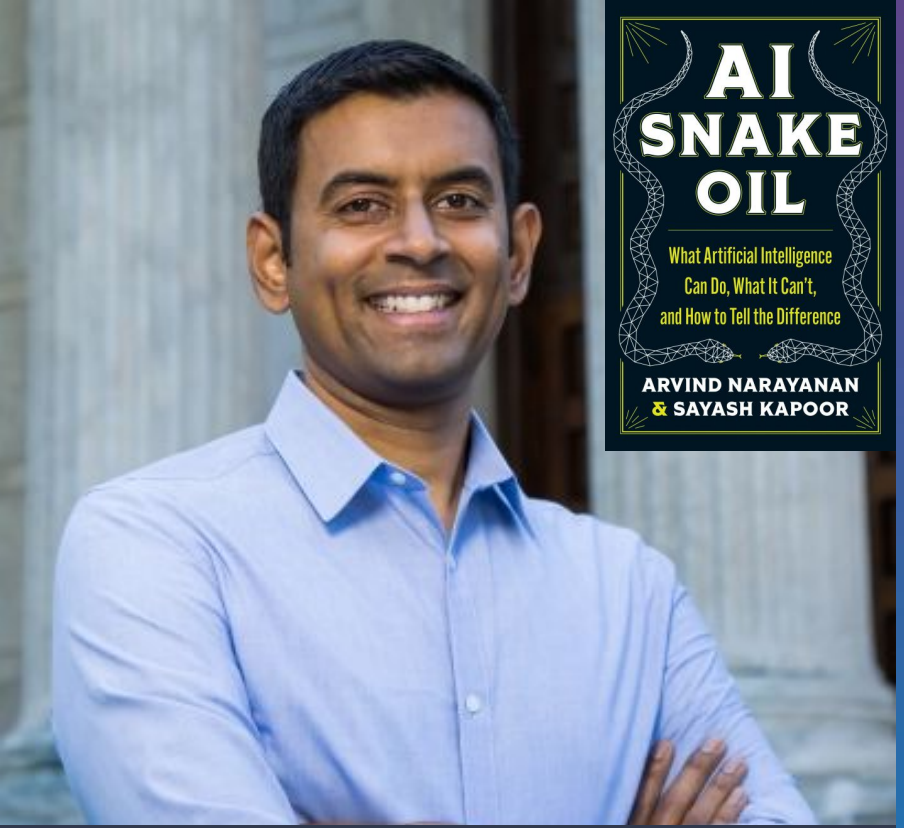
Alphonsus Gabriel Capone	✓
Scarface	✓
Snorky	✓

Intelligent search

Al Kapone	→	Al Capone
Al Cappone	→	Al Capone
Alc Apone	→	Al Capone

In business life and official affairs, identifying and checking the other party is essential.
We offer a solution based on three main pillars, that is reliable and convenient to implement.

precognox



ARVIND NARAYANAN
Princeton professor,
author of AI Snake Oil, 2024

1.
Real transformation takes decades - **POC trap**

2.
The era of “just scale it” is over

3.
Software might become a service again

“Használd az MI-t arra, amit az emberek nem tudnak megcsinálni”

Babak Rasolzadeh · 1st

AIML @ Apple | Product Leader | Startup Advisor | PhD in Computer Vision and Robotics

Top Artificial Intelligence (AI) Voice

San Francisco Bay Area · Contact info

Apple

KTH Royal Institute of Technology

Get In Touch

ENDRE JOFOLDI

CEO, Precognox Ltd.

endre.jofoldi@precognox.com

+36 20 886-13-91

precognox