EVIDEN

Kybernetické hrozby AI v medicínskom rozhodovaní

Jarná ITAPA 2024

Michal Sekula
19.6.2024

an atos business

EVIDEN

Skutočnosť alebo fikcia?

Test výkonnosti modelu umelej inteligencie ChatGPT na testoch USMLE

Štúdia publikovaná v PLOS Digital Health, február 2023

USMLE

- skúška na lekársku licenciu v USA
- pozostáva zo 3 stupňov Step 1, Step 2CK a Step 3

ChatGPT

- bez špecializovaného vstupu od trénerov

Výsledok

- blížil sa alebo dosahoval hranicu na absolvovanie skúšok, tj. 60%
- ukázal čiastočnú schopnosť extrahovať nezvyčajné a novátorské prístupy

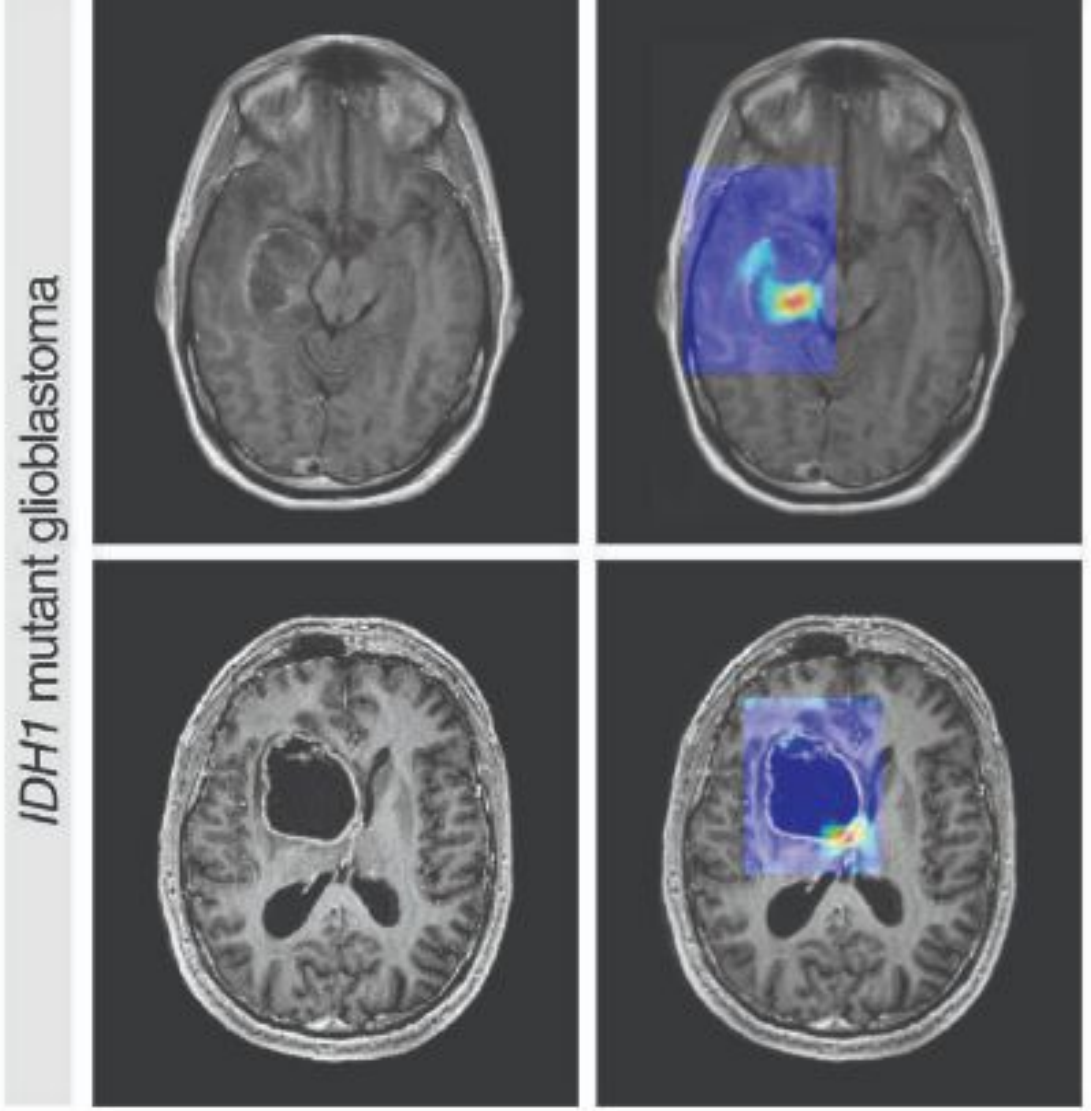
https://journals.plos.org/digitalhealth/article?id=10.1371/journal.pdig.0000198

EVIDEN

EVIDEN

Výhody AI v medicínskom rozhodovaní

- **Analýza obrazových materiálov (RTG, CT..**



A deep learning algorithm trained to analyze images from MRI scans predicts the presence of an *IDH1* gene mutation in brain tumors.

Credit: CA Cancer J Clin March/April 2019. doi: 10.3322/caac.21552. CC BY 4.0.

EVIDEN

Výhody AI v medicínskom rozhodovaní

- **Analýza veľkých objemov dát a hľadanie vzorcov**

EVIDEN

Výhody AI v medicínskom rozhodovaní

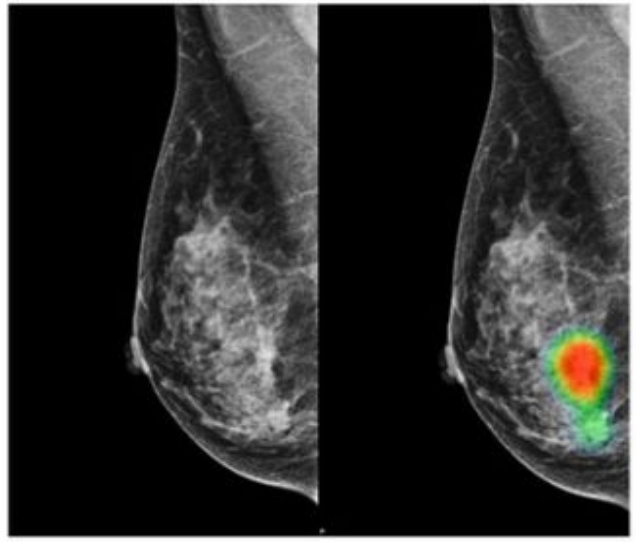
- **Zvýšená presnosť diagnostiky**

Healthcare IT News

AI helps radiologists improve accuracy in breast cancer detection with lesser recalls

According to the study, the AI alone showed 88.8% sensitivity in breast cancer detection, whereas radiologists alone showed 75.3%. When radiologists were aided by AI, the accuracy increased by 9.5% to 84.8%.

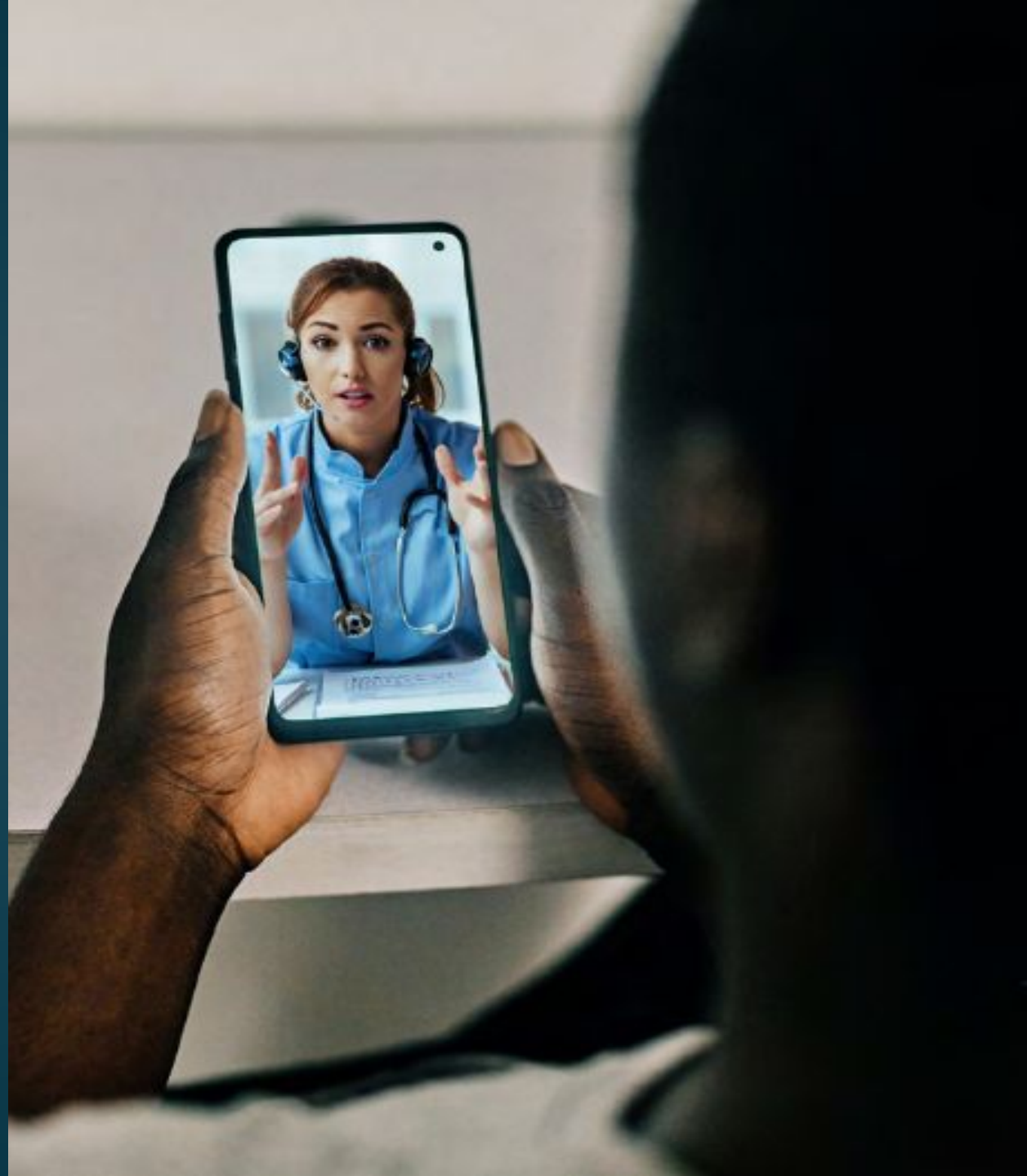
By Dean Koh | February 11, 2020 | 09:33 PM



EVIDEN

Výhody AI v medicínskom rozhodovaní

- **Prediktívna analýza na prevenciu chorôb**



EVIDEN

Výhody AI v medicínskom rozhodovaní

- **Zefektívnenie prevádzky**

EVIDEN

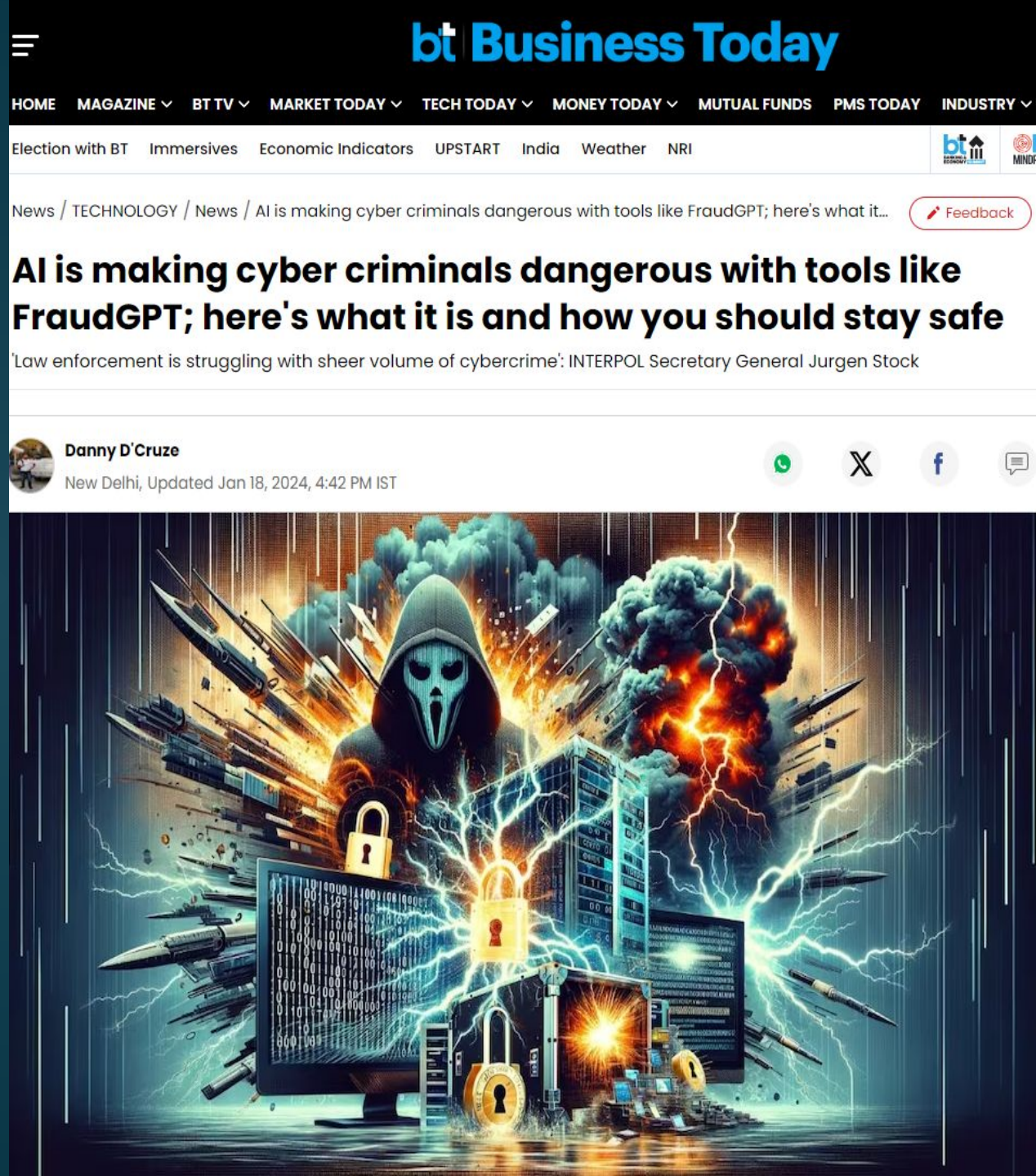
Kybernetické útoky využívajúce AI

Používanie pokročilých algoritmov strojového učenia na identifikáciu slabých miest, predpovedanie vzorov a využívanie slabých stránok

Efektívnosť a rýchla analýza údajov zvyšuje schopnosť hackerov k rýchlemu prieniku alebo škodám.

Tradičné metódy kybernetickej bezpečnosti už nestačia, pretože kybernetické útoky AI sa prispôsobujú a vyvíjajú v reálnom čase.

Forbes, marec 2024



EVIDEN

Kybernetické hrozby

Neoprávnený prístup k citlivým údajom

Útoky na nemocničnú infraštruktúru

Útoky vedúce k nesprávnej diagnóze a liečbe

- manipulácia s lekárskymi údajmi
- útoky na algoritmy a manipulácia s modelmi AI

Kybernetická ochrana – výzvy modernej doby

Kyberbezpečnostné hrozby

- Cyberattacks
- Geopolitical Threats
- Threats Posed by Deepfake Technology
- Cloud-Based Cyber Threats
- IoT Vulnerabilities
- Third-Party Cyber Threats
- More Intelligent Social Engineering Attacks
- Mobile Security Threats
- AI-Enhanced Cyber Threats
- Shortage of Skilled Cybersecurity Professionals

Kybernetická ochrana

- Cloud
- Network
- Endpoint
- Identity
- Exposure Management
- SIEM/XDR
- Apps
- Database
- Vulnerability
- Industry Solutions

Moderná nemocnica

Možné technologické riešenie

1000+ Rules and Signatures

200+ Threat Intel Sources

100+ Machine Learning Models

24x7 SOC Monitoring for known threats

24x7 Threat Intelligence for known attackers

24x7 Threat Hunting for unknown threats/attackers

EVIDEN

Managed Detection and Response

Fight back with Gen AI: AIsaac Cyber Mesh

EVIDEN

an atos business

Ďakujem

michal.sekula@eviden.com