

Medizinische KI mit Datenschutz

[Originalartikel](#)

[Backup](#)

<html> <p class=„printversionback-to-article printversion-hide“><a href=„<https://www.heise.de/tr/artikel/Medizinische-KI-mit-Datenschutz-4428179.html>“>zurück zum Artikel</p><figure class=„printversionlogo“><svg preserveaspectratio=„xMinYMin“ xmlns=„<http://www.w3.org/2000/svg>“ viewBox=„0 0 600 190“ width=„180“ height=„57“><path d=„M398.25,125.73H379.5L370,169.45l-8.47-43.73H342.22l-9.3,43.35-8.62-43.35h-19l16.88,62H342l9.15-41.4,9.07,41.4h19.65Zm-92.17,34.8v-.83c0-17.25-7.87-35.93-31.12-35.93-24.22,0-31.87,18.52-31.87,34.13,0,20.1,12.45,32.1,31.35,32.1,12.83,0,23.85-6.15,30.9-17.92l291.53,165a16.5,16.5,0,0,1-15.67,11c-8.47,0-14.17-6.45-14.17-14.7v-.67h44.4ZM274.8,136.9c7.5,0,12.15,5.33,12.38,12.23H261.75c83-5,4.35-12.23,13-12.23M217.42,97.6h18.15v16.27H217.42Zm0,28.2h18.15v62H217.42Zm-5.25-.07H193.42L183.15,167.8l-11-42.07H152.77l20.18,62h19.13ZM154,160.53v-.83c0-17.25-7.87-35.93-31.12-35.93C98.63,123.77,91,142.3,91,157.9,91,178,103.43,190,122.33,190c12.83,0,23.85-6.15,30.9-17.92l-13.73-7.2a16.5,16.5,0,0,1-15.67,11c-8.48,0-14.17-6.45-14.17-14.7v-.67Zm-31.2-23.62c7.5,0,12.15,5.33,12.38,12.23H109.72c75-5,4.35-12.23,13.05-12.23m-50.7,17.33c8.7-3.67,16.43-9.37,16.43-23.17,0-23-19.95-27.23-31.87-27.23H21.15v83.85h19V157.75H52.95l16,29.92h21.6Zm-15.52-12H40.05v-22.8H56.7c3.52,0,13.05,23,13.05,11.17,0,2.63-1.8,11.63-13.2,11.63M600,22H580.57l-10.2,44.4L560.18,22H540.75l18,58.28c1,3,1.28,4.27,1.28,5.93,0,2.1-1.2,4.5-6.68,4.5h-9.6V105.3H559.2c5.47,0,9.15-.67,12.9-4.73,3.22-3.45,4.65-7.2,6.07-11.62Zm-82.05,29.1c0,6.3-.6,16.12-11.4,16.12-9.9,0-11.55-7.95-11.55-16.72,0-3.96-15.9,11.18-15.9s11.77,8.7,11.77,16.5m1-29v5.7c-3.3-3.22-8.18-6.75-17.18-6.75C486.9,21,476.1,32.78,476.1,51.23c0,24.07,15.53,29.93,25.65,29.93,8.32,0,12.07-2.62,16.28-5.32v8.4c0,7-4.05,9.82-10.8,9.82-9.53,0-11.25-4.8-11.25-8.93H477.15v.75c0,13.5,11.63,20.25,28.35,20.25,20.18,0,30.75-7.58,30.75-23.7V22ZM437.7,20C414.53,20,405,36.82,405,52.5c0,24.45,17.1,33.3,33.3,33.3,20.78,0,33.38-12.82,33.38-32.93,0-14.85-8-32.92-34-32.92m.83,51.23c-10.72,0-15.07-8.18-15.07-18.53,0-13,7.28-18.15,14.18-18.15,10,0,15.6,5.85,15.6,19-.08,9.23-4.58,17.63-14.7,17.63M380.33,0h18.15V83.93H380.33ZM340,20c-23.17,0-32.7,16.87-32.7,32.55,0,24.45,17.1,33.3,33.3,33.3,20.78,0,33.38-12.82,33.38-32.93C374,38,366,20,340,20m.83,51.23c-10.72,0-15.08-8.18-15.08-18.53,0-13,7.28-18.15,14.17-18.15,10,0,15.6,5.85,15.6,19-.07,9.23-4.57,17.63-14.7,17.63M300.9,83.93V39.3c0-12.6-6.67-19-19.28-19-8.7,0-14.47,3.45-17.47,7V21.75H245.63v62h18.3V49.2c0-8.32,1.2-14.25,9.6-14.25,7.35,0,9.48,9,10.72V83.92Zm-65.18,0V41.47c0-13.2-6.9-21.3-19.72-21.3-3.6,0-11.83-17.7,8.33V0H180V83.93h18.3V51.23c0-9.75,2.25-15.45,9.9-15.45,9,0,9.38,8.18,9.38,14.63V83.93ZM175.8,69.3,162,62.18c-1.27,3.9-4.87,9.3-12,9.3-10.12,0-13.8-10.8-13.8-18.68,0-7.5,3.45-18.68,13.2-18.68,7.13,0,10.42,5.25,12.15,8.7l13.58-7.72c-8.7-13.8-20.92-15-26.48-15-14,0-31.12,8.47-31.12,33.3,0,23.32,16.27,32.55,30.75,32.55,9.45,0,20.47-4.43,27.52-16.65M113.33,56.7v-.82c0-17.25-7.87-35.93-31.13-35.93C58,19.95,50.33,38.47,50.33,54.07c0,20.1,12.45,32.1,31.35,32.1,12.82,0,23.85-6.15,30.9-17.93l-13.8-7.12a16.5,16.5,0,0,1-15.68,11C74.7,72.15,69,65.7,69,57.38V56.7ZM82.05,33.07c7.5,0,12.15,5.32,12.38,12.22H69c82-5,4.43-12.22,13.05-12.22M58.73,16.5,62.48,0H0V16.5H21.15V83.85h19V16.5Z“ fill=„#ce001e“/></svg></figure><figure class=„aufmacherbild“></figure><p>An der Stanford University läuft der erste große Test, bei dem Maschinenlern-Algorithmen aus Patientendaten lernen, die vor unbefugten Zugriffen geschützt sind.</p><p>KIünstliche Intelligenz-Systeme (KI) können in

der Medizin eine große Hilfe sein und Krankheiten diagnostizieren, ihnen vorbeugen sowie unsere Lebensdauer verlängern. Doch dieses Potenzial hat einen Haken: KI-Algorithmen benötigen riesige Datenmengen zum Lernen, allerdings können medizinische Aufnahmen, genetische Informationen und elektronische Patientenakten sensible persönliche Informationen enthalten. Deshalb arbeiten Forscher der Stanford Medical School gemeinsam mit der University of California (UC) Berkeley, deren Ausgründung Oasis Labs, sowie Wissenschaftlern der ETH Zürich daran, den Lernprozess so abzusichern, dass die Daten nicht in unbefugte Hände geleakt oder anderweitig missbraucht werden können.

Im Rahmen eines Anfang Mai gestarteten groß angelegten Tests können Patienten mit Augenproblemen wählen, ob sie ihre medizinischen Daten dem Training einer KI zur Verfügung stellen wollen. Diese soll Erkrankungen wie diabetische Retinopathie (Netzhautschäden durch zu hohen Blutzucker) und Glaukome (Netzhaut- und Sehnervschäden) anhand von Aufnahmen diagnostizieren lernen, ohne dass die Algorithmen jemals Zugriff auf persönliche Daten haben. Die Patienten geben in einer [App](https://kara.cloud/#/) ophthalmologische Testergebnisse und Daten aus ihrer Krankengeschichte frei.

Chip gesichert

Oasis Labs speichert die privaten Patientendaten auf einem gesicherten Chip, den es zusammen mit der UC Berkeley entwickelt hat. Die Daten bleiben dabei stets innerhalb der Oasis-Cloud. Außerdem entstehende können Algorithmen einspeisen und Ergebnisse erhalten, ohne dass die Daten selbst jemals das System verlassen. Trifft eine Zugriffsanfrage ein, wird [ein sogenannter smarter Vertrag](https://www.heise.de/tr/artikel/Schlaue-Vertraege-voller-Luecken-3986434.html) ausgelöst, also eine Software, die einer Blockchain vorgeschaltet ist. Die Software notiert, wie die Daten verwendet wurden und prüft zudem, ob die Maschinenlern-Programmierung korrekt ausgeführt wurde. „Es ist sehr spannend, dass wir das mit echten Daten testen können, um zu zeigen, dass es funktioniert“, sagt Dawn Song, Mitgründerin von Oasis Labs und Professorin an der UC Berkeley. Je mehr Daten in das Training einfließen, desto genauer werde das System.

Probleme bei der Handhabung privater Patientendaten zeichnen sich schon seit einiger Zeit ab. In vielen Ländern ist es etwa aus rechtlichen Gründen nicht einfach, medizinische Akten für das Trainieren von KI zu nutzen. Selbst wenn es möglich ist, werden in der Regel relativ kleine Datenmengen verwendet, was das Potenzial der Technologie erheblich einschränkt. Das will Oasis Lab nun ändern.

Streng vertrauliche Informationen

Die neue Schutztechnologie könnte es auch einfacher machen, KI auf andere vertrauliche Informationen wie Finanzberichte, die Kaufgewohnheiten von Kunden oder Surfdaten im Internet anzuwenden. Laut Song ist geplant, die medizinischen Anwendungen zu erweitern, bevor auf andere Bereiche verwiesen wird.

Lesen Sie mehr zum Einsatz von KI in der Medizin:

- [Warum erkennen KI-Systeme Menschen mit Behinderung so schlecht?](https://www.heise.de/tr/artikel/Warum-erkennen-KI-Systeme-Menschen-mit-Behinderungen-so-schlecht-4278394.html) [3]
- [KI erkennt Depression](https://www.heise.de/tr/artikel/KI-erkennt-Depression-4271725.html) [4]
- [Lernstoff: So sammeln KI-Trainer Daten für Künstliche Intelligenzen](https://www.heise.de/tr/artikel/Lernstoff-So-sammeln-KI-Trainer-Daten-fuer-Kuenstliche-Intelligenzen-4225614.html) [5]
- [KI erkennt Krebs: Neuronale Netze in der Radiologie](https://www.heise.de/hintergrund/KI-erkennt-Krebs-Neuronale-Netze-in-der-Radiologie-4301435.html) [6]
- [KI im](https://www.heise.de/hintergrund/Dr-Watson-weiss-nicht-weiter-4313834.html)

Gesundheitssystem: Dr. Watson weiß nicht weiter [7]

class=„heiseplus-Ink“
 href=„https://www.heise.de/hintergrund/Der-zweite-Hype-der-Genmedizin-4259471.html“>Der zweite Hype der Genmedizin [8]
 </div> <p>„Es ist eine unglaublich starke Idee, Berechnungen durchzuführen und dabei [sensible] Daten geheim halten zu können“, sagt David Evans von der University of Virginia.</p> <h3 class=„subheading“>Über Krankheitsuser hinweg</h3> <p>Wenn maschinelles Lernen über Krankheitsuser und verschiedene Patientengruppen hinweg angewandt werde, eröffne das völlig neue Möglichkeiten dafür, Krankheiten mit Genomik- und anderen Testergebnissen sowie weiteren Patienteninformationen zu verknüpfen, sagt der Experte für maschinelles Lernen und Sicherheit. „Es wäre schön, wenn Forscher in allen medizinischen Unterlagen nachlesen könnten“, sagt Evans. „Sie könnten analysieren, warum ein Medikament nicht wirkt. Aber das geht heute noch nicht.“</p> <p>Trotz dieser Möglichkeiten gibt sich Evans vorsichtig. Das Speichern von Daten in sicherer Hardware könne zu einem potenziellen Fehler führen. Wenn der Hersteller der Datensicherungs-Hardware gehackt wird, sind alle verarbeiteten Daten gefährdet. Die Sicherheit von Blockchains sei relativ unbewiesen, fügt er hinzu. Bei Oasis Labs' Ansatz „kommen viele verschiedene Technologien zusammen. Einige sind ausgereift, während andere zwar auf dem neuesten Stand sind, aber noch mit Herausforderungen kämpfen.“</p> <hr/><p>URL dieses Artikels:
<small>

http://www.heise.de/-4428179

</small></p> <p>Links in diesem Artikel:
<small>

[1] https://kara.cloud/#/

</small>
<small>

[2] https://www.heise.de/tr/artikel/Schlaue-Vertraege-voller-Luecken-3986434.html

</small>
<small>

[3] https://www.heise.de/tr/artikel/Warum-erkennen-KI-Systeme-Menschen-mit-Behinderungen-so-schlecht-4278394.html

</small>
<small>

[4] https://www.heise.de/tr/artikel/KI-erkennt-Depression-4271725.html

</small>
<small>

[5] https://www.heise.de/tr/artikel/Lernstoff-So-sammeln-KI-Trainer-Daten-fuer-Kuenstliche-Intelligenzen-4225614.html

</small>
<small>

[6] https://www.heise.de/hintergrund/KI-erkennt-Krebs-

Neuronale-Netze-in-der-Radiologie-4301435.html

</small>
<small>

[7] https://www.heise.de/hintergrund/Dr-Watson-weiss-nicht-weiter-4313834.html

</small>
<small>

[8] https://www.heise.de/hintergrund/Der-zweite-Hype-der-Genmedizin-4259471.html

</small>
</p> <p class=„printversion__copyright“>Copyright © 2019 Heise Medien</p> </html>

From:
<https://schnipsl.qgelm.de/> - Qgelm

Permanent link:
<https://schnipsl.qgelm.de/doku.php?id=wallabag:medizinische-ki-mit-datenschutz>

Last update: **2021/12/06 15:24**

