idw - Informationsdienst Wissenschaft
Nachrichten, Termine, Experten

Press release

Lernende Systeme - Die Plattform für Künstliche Intelligenz
Linda Treugut
04/08/2020
http://idw-online.de/en/news744482

Research results
Economics / business administration, Information technology, Medicine, Nutrition / healthcare / nursing, Politics
transregional, national

Patientendaten schützen, Diagnosen verbessern: Sichere KI in der Medizin

Künstliche Intelligenz (KI) kann die Gesundheitsversorgung der Menschen verbessern. Intelligente Assistenzsysteme unterstützen Ärztinnen und Ärzte bei Prävention, Diagnose sowie Therapie-Entscheidungen. Voraussetzung: der Schutz der Patientendaten und die Sicherheit der KI-Systeme ist gewährleistet. In ihrem aktuellen Whitepaper untersuchen Experten der Plattform Lernende Systeme das Datenmanagement und die IT-Sicherheit beim Einsatz von KI in der Medizin und adressieren Gestaltungsoptionen. Sie fordern unabhängige Prüfstellen, die die KI-Systeme zertifizieren, und Kontrollmechanismen, die nur berechtigten Personen den Zugriff auf sensible Daten erlauben.

München, 08. April 2020 – KI-basierte Assistenzsysteme in Arztpraxen und Kliniken bietet viele Chancen für das Gesundheitswesen. Mithilfe der intelligenten, selbstlernenden Systeme können Ärztinnen und Ärzte frühzeitige Diagnosen stellen, individuelle Therapien entwickeln und ihre Entscheidungen auf eine breite Informationsbasis stützen. Grundlage der KI-Systeme sind Daten. "Nur wenn genügend nutzbare Daten verfügbar sind, kann die Gesellschaft vom Potential der KI in der Medizin profitieren. Auf der anderen Seite sind die Daten gleichsam die Achillesferse der Assistenzsysteme und bedeuten eine große Herausforderung für ihre Sicherheit", erklärt Jörn Müller-Quade, Professor für Kryptographie und Sicherheit am Karlsruher Institut für Technologie (KIT) und Leiter der Arbeitsgruppe IT-Sicherheit, Privacy, Recht und Ethik in der Plattform Lernende Systeme. Fehlerhafte oder bewusst verfälschte Trainingsdaten können in der Diagnostik dazu führen, dass das KI-System falsche Ergebnisse liefert. Fehlbehandlungen und physische oder psychische Belastungen können die Folge derartiger Datenmanipulationen sein. Auch Angriffe auf die KI-Software und -Datenbanken können nach Ansicht der Autoren falsche Diagnosen und Behandlungsempfehlungen verursachen. Vor allem die sensiblen Patientendaten bedürfen eines besonderen Schutzes vor Missbrauch.

Um den Einsatz der KI-Systeme in der Medizin sicher und zum Wohle der Patienten zur gestalten, empfehlen die Autoren unter anderem der Zertifizierung der KI-Systeme – etwa für die Sicherstellung unverfälschter Trainingsdaten. Wichtig ist hier, gemeinsame Leitlinien und Prüfvorschriften für die Zulassung und Zertifizierung für KI-Datenbanken sowie für deren Betreiber zu entwickeln. Darüber hinaus sollten Hersteller gesetzlich zur Mängelbehebung verpflichtet und neutrale Einrichtungen mit dem Betrieb des KI-Assistenzsystems beauftragt werden. Ein unabhängiges Prüfkomitee kann zudem in regelmäßigen Abständen die Funktionsweise der zertifizierten und eingesetz¬ten KI-Systeme überprüfen und Rückrufprozesse können etabliert werden.

Zum Schutz vor Hacker-Angriffen auf das KI-System oder vor unerlaubtem Zugriff auf die Gesundheitsdaten der Menschen empfehlen die Autoren besondere Kontrollmechanismen. "Die Einführung der elektronischen Patientenakte ist einer der Grundvoraussetzungen für ein selbstlernendes KI-Assistenzsystem", so Jörn Müller-Quade. "Neben den grundlegenden Gesundheitsdaten der Menschen sollte die ePA auch Informationen zu Allergien, Diäten oder Krankengymnastik bereithalten und damit deutlich mehr Akteure als bislang einbeziehen. Zu klären sind die Rechte und Pflichten dieser Akteure und ihr Zugriff auf die Patientendaten muss entsprechend zeitlich und inhaltlich begrenzt werden." Besonders wichtig ist für die Autoren, dass Patientinnen und Patienten ihre Daten, die in der ePA gespeichert sind, nach einer medizinischen Behandlung freiwillig und geschützt für Forschungszwecke zur Verfügung stellen und

damit zur Verbesserung KI-basierter Diagnosen und Therapien beitragen können.

Um die Patientendaten zu schützen, schlagen die Autoren einen kombinierten Sicherheitsansatz vor. So solle erstens der Datenverkehr verschlüsselt, integritäts- und authentizitätsgesichert sein. Zweitens solle stets eine Authentisierung der Kommunikationspartner stattfinden, sodass nur autorisierte Personen Zugriff auf das System haben und Manipulationen mittels kryptographischer Verfahren, wie zum Beispiel Verschlüsselung und Signaturen, verhindert werden, heißt es in dem Whitepaper. Zur Authentisierung benötigen Ärztinnen und Ärzte ihren Heilberufsausweis, die elektronische Gesundheitskarte (eGK) der Patientin oder des Patienten sowie die zugehörige PIN.

Über die Nutzung der eigenen Gesundheitsdaten müssen die Menschen souverän bestimmen können. Die elektronische Gesundheitskarte (eGK) gilt dafür als zentrales technisches Instrument. Die Krankenkassen als ausgebende Stellen sollten die Sperrung der eGK ermöglichen, um so einen unautorisierten Zugriff auf Daten zu verhindern. Ergänzend schlagen die Autoren als Rückfall-Lösung einen Minimalmodus vor, in dem die wichtigsten Funktionen der Gesundheitskarte aufrechterhalten werden, beispielsweise wenn die Patientin oder der Patient seine PIN vergessen hat.

Über das Whitepaper
Das Whitepaper „Sichere KI-Systeme für die Medizin“ zeigt das Potenzial sowie die Herausforderungen beim Einsatz von KI-basierten Assistenzsystemen in der Gesundheitsversorgung. Die Autoren beleuchten die Dateninteraktionen und erläutern die sicherheitsrelevanten Aspekte. Daraus leiten sie Gestaltungsoptionen ab, wie sichere KI-Systeme in der Medizin Realität werden können. Die Analyse basiert auf dem Anwendungsszenario „Mit KI gegen Krebs“, mit dem die Arbeitsgruppe Gesundheit, Medizintechnik, Pflege in der Plattform Lernende Systeme zeigt, wie Künstliche Intelligenz in naher Zukunft die Heilungschancen für Krebspatienten verbessern kann. Das Whitepaper wurde von Mitgliedern der Arbeitsgruppe IT-Sicherheit, Privacy, Recht und Ethik mit Unterstützung der Arbeitsgruppe Gesundheit, Medizintechnik, Pflege verfasst. Es steht zum Download zur Verfügung unter
https://www.plattform-lernende-systeme.de/files/Downloads/Publikationen/AG3_6_Whitepaper_07042020.pdf

Über die Plattform Lernende Systeme
Die Plattform Lernende Systeme wurde 2017 vom Bundesministerium für Bildung und Forschung (BMBF) auf Anregung des Fachforums Autonome Systeme des Hightech-Forums und acatech gegründet. Sie vereint Expertinnen und Experten aus Wissenschaft, Wirtschaft, Politik und Zivilgesellschaft aus dem Bereich Künstliche Intelligenz. In Arbeitsgruppen entwickeln sie Handlungsoptionen und Empfehlungen für den verantwortlichen Einsatz von Lernenden Systemen. Ziel der Plattform ist es, als unabhängiger Makler den gesellschaftlichen Dialog zu fördern, Kooperationen in Forschung und Entwicklung anzuregen und Deutschland als führenden Technologieanbieter für Lernende Systeme zu positionieren. Die Leitung der Plattform liegt bei Bundesministerin Anja Karliczek (BMBF) und Karl-Heinz Streibich (Präsident acatech).

URL for press release:
https://www.plattform-lernende-systeme.de/files/Downloads/Publikationen/AG3_6_Whitepaper_07042020.pdf

Experten der Plattform Lernende Systeme untersuchen im aktuellen Whitepaper "Sichere KI-Systeme in der Medizin" das Datenemanagement und die IT-Sicherheit beim Einsatz von KI in der Medizin.
Plattform Lernende Systeme