

Wie Künstliche Intelligenz den Datenschutz verbessert: Forschende der Hochschule Hamm-Lippstadt stellen Ergebnisse in Belgien vor

Wie kann Künstliche Intelligenz (KI) den Schutz persönlicher Daten im Netz optimieren? Dieser Frage gingen Navid Ashrafi, wissenschaftlicher Mitarbeiter an der Hochschule Hamm-Lippstadt (HSHL), und Prof. Dr.-Ing. Jan-Niklas Voigt-Antons, Lehrgebiet „Angewandte Informatik mit Schwerpunkt Immersive Medien“ an der HSHL, mit Kolleg*innen von der Technischen Universität Berlin und dem Deutschen Forschungszentrum für künstliche Intelligenz nach. Das Ergebnis der Forschungsarbeit haben sie am Mittwoch, den 21. Juni 2023 auf der 15. International Conference on Quality of Multimedia Experience (QoMEX) in Gent, Belgien, vorgestellt.

Grundsätzlich gilt: Der Schutz privater Daten ist für eine positive Nutzer*innenerfahrung und Akzeptanz von IT-gestützten Dienstleistungen und Anwendungen von größter Bedeutung, insbesondere im Gesundheitsbereich, in dem mit besonders sensiblen Daten gearbeitet wird. Doch sogar die gängigen Anonymisierungstechniken bieten nicht immer vollständigen Schutz, da sie anfällig für eine Re-Identifizierung der Nutzer*innen sein können. Abhilfe schafft die Erstellung sogenannter synthetischer Daten, die aktuell die Anonymisierung schrittweise ersetzen.

KI und Datenschutz: Rauschen macht Benutzer*innen anonym

„Synthetische Daten sind Daten, die von Computern synthetisch generiert werden, basierend auf einem realen Datensatz, zum Beispiel Text- oder Bilddaten. Die realen Daten werden als Trainingsdaten für ein maschinelles Lernverfahren verwendet, das die Verteilung der Daten lernt und darauf basierend ähnliche Beispiele generiert“, erklärt Prof. Voigt-Antons. Das geschieht zum Beispiel mit sogenannten Generative Adversarial Networks (GANs).

Die meisten neuen Versionen dieser Netzwerke zielen darauf ab, die Qualität der erzeugten Daten zu verbessern und die Privatsphäre der echten Trainingsdaten zu schützen. „Neue GANs zur Wahrung der Privatsphäre integrieren differentielle Datenschutzstandards“, sagt Navid Ashrafi. „Das bedeutet, dass ein Rauschen zu den Informationen hinzugefügt wird, wodurch die Wiedererkennung von Benutzer*innen in den echten Daten erschwert wird.“

Medizinischer Bereich wird profitieren

Auch wenn die Entwicklung und das Wachstum dieser KI-Netzwerke von den Fortschritten der Künstlichen Intelligenz im Allgemeinen abhängt, ist sich Prof. Voigt-Antons sicher, dass diese Verfahren mehr und mehr in Bereichen Einzug halten werden, in denen die Wahrung der Privatsphäre besonders wichtig ist. „Der gesamte medizinische Bereich wird daher ein besonders prominentes Anwendungsgebiet werden“, so der HSHL-Professor. Für seine Arbeit hat Navid Ashrafi den „Diversity and Societal Impact“-Award der QoMEX erhalten.

Weitere Informationen:

<https://qomex.org/>

Prof. Dr.-Ing. Kira Kastell
Präsidentin

Marc Bracht
Kommunikation und Marketing
marc.bracht@hshl.de

Johanna Bömken
Leiterin Kommunikation und Marketing

Fon +49 2381 8789 - 105
johanna.boemken@hshl.de

Lippstadt/Gent, 22.06.2023

Postanschrift
Hochschule Hamm-Lippstadt
University of Applied Science
Marker Allee 76 – 78
59063 Hamm

Besucheradresse
Gebäude H 2.1
Marker Allee 76 – 78
59063 Hamm

Web
hshl.de

Über die Hochschule Hamm-Lippstadt:

Die Hochschule Hamm-Lippstadt (HSHL) bietet innovative und interdisziplinäre Studiengänge aus den Bereichen Ingenieurwissenschaften, Naturwissenschaften, Informatik und Wirtschaft an. In 14 Bachelor- sowie zehn Masterstudiengängen qualifizieren sich an der HSHL derzeit 5140 Studierende praxisorientiert für den späteren Beruf. An den beiden Campus in Hamm und Lippstadt verfügt die Hochschule über modernste Gebäude und rund 15.000 Quadratmeter Laborfläche für zukunftsorientierte Lehre und Forschung. Für das rund 400-köpfige Team um Präsidentin Prof. Dr.-Ing. Kira Kastell und Kanzlerin Sandra Schlösser bilden besonders Toleranz, Chancengleichheit und Vielfalt die Grundlage für eine Arbeit, die nachhaltig zur gesellschaftlichen Entwicklung beiträgt.

www.hshl.de