PRESS RELEASE

Fending Off Cyberattacks in Healthcare

The BMFTR is providing nearly €2.5 million to fund the "SecureNeuroAI" project, which involves researchers from Bonn and FIZ Karlsruhe

Komm. Vorstandsvorsitzender
Univ.-Prof. Dr. Bernd Weber
Tel: +49 228 287-10900
Fax: +49 228 287-9010900
bernd.weber@ukbonn.de

Kommunikation und Medien

Viola Röser
Leitung

Tel: +49 228 287-10469
viola.roeser@ukbonn.de

Universitätsklinikum Bonn
Kommunikation und Medien
Venusberg-Campus 1
Geb. 02
53127 Bonn

Bonn, July 31– Artificial intelligence (AI) is designed to make our health system even more efficient. Yet cyberattacks are capable not only of jeopardizing patient safety but also impairing medical devices and hindering the work of emergency responders. With the "SecureNeuroAI" project, researchers from the University of Bonn, University Hospital Bonn and FIZ Karlsruhe – the Leibniz Institute for Information Infrastructure are aiming to develop secure, AI-powered methods for detecting medical emergencies in real time using the example of epileptic seizures, although their findings should be applicable to many other areas. The Federal Ministry of Research, Technology and Space (BMFTR) is providing almost €2.5 million in funding over a three-year period.

Everyone is talking about AI, which is increasingly making its presence felt in virtually every area of our lives—and the broad field of healthcare is no exception. Medical devices and applications using AI methods could potentially improve the quality of life for patients. Integrating AI into patient care increases the risk of cyberattacks, however, which are capable not only of jeopardizing patient safety but also hindering the work of emergency responders and stopping medical devices from functioning properly.

The "SecureNeuroAI" project is to receive nearly €2.5 million in funding from the BMFTR over the next three years. Among other things, the aim will be to develop data authentication methods that do not interfere with AI processing of the data, but still allow the origin of this information to be verified.

The project is being coordinated by Professor Elena Demidova, head of the Data Science and Intelligent Systems (DSIS) Working Group at the University of Bonn and a member of the "Modelling" and "Sustainable Futures" Transdisciplinary Research Areas. Elena Demidova's working group brings extensive AI expertise to the project. Also on board are Professor Michael Meier, head of the IT Security Working Group at the University of Bonn's Institute for Computer Science, Professor Björn Krüger from the Department of Epileptology at the University Hospital Bonn, head of the Personalized Digital Health and Telemedicine working group, and Professor Franziska Boehm from FIZ Karlsruhe.

The researchers involved in SecureNeuroAI are working toward developing secure, AI-powered methods for detecting medical emergencies in real time, taking epileptic seizures as their example. The detection is based on a comprehensive analysis and the logging of multimodal sensor data. This is done using, for instance, wearable electronic devices

("wearables" for short) that record vital parameters such as heart and respiratory rate as well as patients' clinical data.

Cyber-secure AI models

The information thus obtained is analyzed using cyber-secure AI models designed to spot seizures and distinguish them reliably from potential cases of data manipulation. At the same time, the project team is setting out technical, organizational and legal measures to help enable these AI methods to be applied in clinical and domestic settings.

The DSIS working group, led by Prof. Dr. Elena Demidova from the University of Bonn, plays a key role in developing AI methods for authenticating the data and developing explainable AI models for manipulation and seizure detection. "AI models are fueled by and highly dependent on the data, making the development of protection mechanisms, such as data authentication and manipulation detection, critical," says Professor Demidova. "In particular, in the area of the AI-driven detection of medical emergencies, manipulation detection poses a significant challenge due to the complexity of the relevant patterns and the scarcity of available data."

The University Hospital Bonn (UKB) plays a central role in the clinical validation and integration of the AI models developed. As an application partner, the Clinic and Polyclinic for Epileptology systematically collects multimodal data for seizure detection and processes it under clinical conditions in order to create a realistic data basis for the AI models. "Artificial intelligence is set to play an ever-greater role in analyzing clinical data," Professor Krüger says. "A secure system mindset is essential, especially in the healthcare sector, where we're working with ultra-sensitive patient data—and it's precisely here that the 'SecureNeuroAI' project comes in."

The working group led by Prof. Dr. Michael Meier from the University of Bonn brings extensive experience in current IT security research topics to the table. "We know from studies on cybersecurity that networked medical devices themselves, but especially the accompanying infrastructure, have vulnerabilities that can enable undetected manipulation of sensor data," says Professor Meier, who is also a member of the transdisciplinary research areas "Modeling," "Individuals & Societies," and "Sustainable Futures" at the University of Bonn.

The Intellectual Property Rights (IGR) research department at FIZ Karlsruhe (FIZ), headed by Prof. Dr. Franziska Boehm, analyzes data protection and IT regulations as well as legal issues concerning artificial intelligence. The aim is to derive recommendations for social processes and digital science, including its infrastructure facilities.

Aiming to protect AI models and data from manipulation

The findings from the project are designed to go a long way toward strengthening the cybersecurity of critical medical devices that use AI methods to detect life-threatening situations in real time. These new technical solutions are intended to enable both AI models and the data underpinning them to be protected against manipulation. The plan is for the findings to be applicable to many other areas besides detecting epileptic seizures and for the project to lay the technological foundations for significantly improving the integrity, availability and reliability of AI-based medical equipment.

Images:

Picture credits: BMFTR

Contacts:

Prof. Elena Demidova
Data Science and Intelligent Systems Group (DSIS)
University of Bonn
Phone +49 (0)228/7369560
Email: elena.demidova@cs.uni-bonn.de

Prof. Dr. Michael Meier
IT Security
University of Bonn
Fraunhofer FKIE
Tel. +49 (0)228/7354249
Email: mm@cs.uni-bonn.de

Prof. Björn Krüger
Department of Epileptology
University Hospital Bonn
Phone +49 228 28751704
Email: bkrueger@uni-bonn.de

Prof. Dr. Franziska Boehm
Vice President Intellectual Property Rights

FIZ Karlsruhe – Leibniz Institute for Information Infrastructure GmbH
Karlsruhe Institute of Technology
Tel. +49 (0)7247/808401
Email: franziska.boehm@fiz-karlsruhe.de

Zum Universitätsklinikum Bonn: Im UKB finden pro Jahr etwa 500.000 Behandlungen von Patient*innen statt, es sind ca. 9.500 Mitarbeiter*innen beschäftigt und die Bilanzsumme beträgt 1,8 Mrd. Euro. Neben den 3.500 Medizin- und Zahnmedizin-Studierenden werden pro Jahr 550 Personen in zahlreichen Gesundheitsberufen ausgebildet. Das UKB steht in der Focus-Klinikliste auf Platz 1 unter den Universitätsklinika (UK) in NRW, hatte in 2023 in der Forschung über 100 Mio. Drittmittel und weist den zweithöchsten Case Mix Index (Fallschweregrad) in Deutschland auf. Das F.A.Z.-Institut hat das UKB mit Platz 1 unter den Uniklinika in der Kategorie „Deutschlands Ausbildungs-Champions 2024“ ausgezeichnet.