

# A U S H A N G

---

## FREIE UNIVERSITÄT BERLIN

Fachbereich Mathematik und Informatik

Promotionsbüro, Arnimallee 14, 14195 Berlin

# D I S P U T A T I O N

**Freitag, 18. Juli 2025, 12:00 Uhr**

**Ort: Seminarraum 049**

**(Fachbereich Mathematik und Informatik, Takustr. 9, 14195 Berlin)**

**Disputation über die Doktorarbeit von**

**Wenjie Huo**

**Thema der Dissertation:**

**Machine Learning in Industry: Applications and Security Challenges**

**Thema der Disputation:**

**From Practical Applications to Security Solutions of Machine Learning**

Die Arbeit wurde unter der Betreuung von **Prof. Dr. K. Wolter** durchgeführt.

Abstract: Machine Learning (ML) has become a key driving factor for innovation in industrial systems, providing powerful tools for automation, monitoring, and quality control. In this talk, I will explore two aspects of ML: its practical applications in industrial environments such as laser beam welding, and the associated security challenges.

On the application side, we investigate the use of spatiotemporal models—including 3D Convolutional Neural Networks (3D-CNN) and CNN-LSTM architectures—for detecting solidification cracks in untrimmed welding videos. In addition, we develop an encoder-decoder-based model for strain estimation, which enables faster and more efficient predictions.

On the security side, ML models remain vulnerable to various types of attacks. This talk focus on one particularly threat—the backdoor attack. I will demonstrate a backdoor attack targeting the crack detection system by exploiting a common phenomenon—illumination. Finally, I will introduce a novel defense strategy designed to counter such threats.

Die Disputation besteht aus dem o. g. Vortrag, danach der Vorstellung der Dissertation einschließlich jeweils anschließenden Aussprachen.

**Interessierte werden hiermit herzlich eingeladen**

Der Vorsitzende der Promotionskommission

Prof. Dr. K. Wolter