Haibo Zhang, Ph.D.

Assistant Professor

Kyushu Institute of Technology
680-4 Kawazu, Iizuka-shi
Fukuoka, Japan

Phone: +81(50)1803-4605
Email: haiboz0105@gmail.com
Website: https://haiboz0105.github.io/homepage/

POSITION

Assistant Professor	Department of Artificial Intelligence Kyushu Institute of Technology, Japan	April 2024-present

EDUCATION

Ph.D.	Kyushu University, Japan Informatics *Supervisor: Prof. Kouichi Sakurai*	March 2024
M.S.	University of Southern California, the United States Cyber Security *Prof. Clifford Neuman*	May 2018
B.S.	Anhui University, China Software Engineering	June 2015

RESEARCH INTERESTS

- **Machine Learning Security:** Protect machine learning systems from various security threats by developing robust algorithms that ensure data integrity and user privacy.
- **Adversarial Attacks and Defenses:** Enhance the robustness of machine learning models against malicious inputs designed to compromise model accuracy and functionality.
- **Image Recognition and Processing:** Develop algorithms that enable computers to interpret and process images, improving the performance of applications such as autonomous driving and medical diagnostics.
- **Machine Unlearning:** Examine how to efficiently train models on extensive datasets and remove specific data when necessary, adhering to privacy requirements without retraining from scratch.

RESEARCH EXPERIENCE

Research Assistant April 2019–March 2022

Strategic International Collaborative Research Program

Joint program with Cyber Security Center, Kyushu University

- Designed and conducted a study to explore the cyber security threats on IoT space, including the blockchain and supply chain applications.
- Published 3 peer-reviewed conference papers and 1 journal manuscript.

FELLOWSHIPS, AWARDS, AND HONORS

- Excellent member, Summer Social Practice, Anhui University — Oct. 2012
- Excellent Group Award, 3rd China Innovative & Entrepreneurship Competition Committee — Aug. 2014
- Outstanding student leader, Anhui University — Sept. 2014
- Chinese College Students Entrepreneur Award (Group Award), China National Computer Congress — Oct. 2014
- Outstanding student award, Kyushu University — March 2024

PROFESSIONAL AFFILIATIONS

- IEEE — 2024-present
- IEEE Women in Engineering — 2024-present
- Information Processing Society of Japan — 2024-present

PROFESSIONAL SERVICE

Manuscript Reviewer

- IEEE Access — Aug. 2021-present
- The Pacific Rim International Conference on Artificial Intelligence — Nov. 2023
- Artificial Intelligence Review — Jun. 2024-present
- IEEE Transactions on Emerging Topics in Computational Intelligence — Jan. 2024-present

PUBLICATIONS

Refereed Journal Articles

1. Zhang, H., & Sakurai, K. (2021). A Survey of Software Clone Detection From Security Perspective, in IEEE Access, vol. 9, pp. 48157-48173, doi: 10.1109/ACCESS.2021.3065872.
2. Zhang, H., & Sakurai, K. (2021). Conditional Generative Adversarial Network-Based Image Denoising for Defending Against Adversarial Attack. IEEE Access, 9, 169031-169043.
3. Zhang, H., Nakamura, T., Isohara, T., & Sakurai, K. (2023). A Review on Machine Unlearning. SN Computer Science, 4(4), 337.
4. Teng MKK, Zhang H, Saitoh T. LGNMNet-RF: Micro-Expression Detection Using Motion History Images. Algorithms. 2024; 17(11):491. https://doi.org/10.3390/a17110491.

Non-Refereed Journal Articles

1. Zhang, H., Yao, Z., & Sakurai, K. (2024). Versatile Defense Against Adversarial Attacks on Image Recognition. arXiv preprint arXiv:2403.08170.

Conference Proceedings

1. Zhang, H., Nakamura, T. and Sakurai, K. (2019). Security and Trust Issues on Digital Supply Chain. The 4th IEEE Cyber Science and Technology Congress (CyberSciTech2019). (International)
2. Zhang, H., Sakurai, K. (2020). Blockchain for IoT-Based Digital Supply Chain: A Survey. The 8th International Conference on Emerging Internet, Data & Web Technologies (EIDWT-2020). (International)
3. Zhang, H., Sakurai, K. (2021). Zero Trust for Supply Chain Security. The 2021 IEEE Conference on Dependable and Secure Computing (poster). (International)
4. Zhang, H., Yao, Z., & Sakurai, K. (2023). Eliminating Adversarial Perturbations Using Image-to-Image Translation Method. In International Conference on Applied Cryptography and Network Security (pp. 601-620). Cham: Springer Nature Switzerland. (International)
5. Zhang, H., Yao, Z., & Sakurai, K. (2023). POSTER: A Fine-Grained Metric for Evaluating the Performance of Adversarial Attacks and Defenses. In International Conference on Applied Cryptography and Network Security (pp. 690-694). Cham: Springer Nature Switzerland. (International)
6. He, P., Zhang, H., Feng, Y. and Sakurai, K. (2023). A Design of Network Attack Detection Using Causal and Non-Causal Temporal Convolutional. The 5th International Conference on Science of Cyber Security (SciSec 2023). (International)
7. Zhang, H., Sakurai, K. (2024). Experimental Exploration of the Power of Conditional GAN in Image Reconstruction-Based Adversarial Attack Defense Strategies. In: Barolli, L. (eds) Advanced Information Networking and Applications. AINA 2024. Lecture Notes on Data Engineering and Communications Technologies, vol 201. Springer, Cham. (International)

Manuscripts in Progress and Under Review

1. Cai, X., Zhang, H., & Koide, H., EDLTXGB: Ensemble Deep Learning Tree-based Detection Method on Various Exfiltration for Advanced Persistent Threats. *Under Review at IEEE Access*
2. Xiang, W., Zhang, H., & Sakurai, K., Component-wise Evaluation of Pixel Deflection: Assessing Its Robustness against Adversarial Attacks. *In Progress*
3. Zhang, H., Yao, Z., Sakurai, K., & Saitoh T., Leveraging the Generalizability of Image-to-Image Translation for Enhanced Adversarial Defense. *In Progress*
4. Kumar, P., Gamini, G., Seal, A., Mohanty, S., Zhang, H., & Sakurai, K., Fooling A Deep Learning-based Facial Expression Recognition System using its Class Activation Map and Differential Evolution. *In Progress*