YIHE ZHANG, PH.D.

EMAIL: yihe.zhang@louisiana.edu **PHONE:** +1 (412)-726-1578
OFFICE: 301 E. Lewis Street, Lafayette, LA 70503, University of Louisiana at Lafayette, USA
HOMEPAGE: https://ihozh.github.io/

RESEARCH INTEREST

Data-Driven Security, Societal Safety, AI Security and Privacy, and AI for Social Good

EDUCATION

University of Louisiana at Lafayette Jan 2018 - May 2024
Ph.D. in Computer Science *Advisor: Dr. Nian-Feng Tzeng*

Carnegie Mellon University Aug 2015 - Jul 2016
Master in Electrical and Computer Engineering

Sun Yat-sen University Aug 2014 - Jul 2015
Master in Computer Engineering *Advisor: Dr. Yinliang Xu*

Sun Yat-sen University Aug 2010 - Jul 2014
Bachelor in Automation

PROFESSIONAL EXPERIENCE

From Jul 2024 – present: Cybersecurity Research Scientist, Informatics Research Institute, University of Louisiana at Lafayette. *Advisor: Dr. Xiali (Sharon) Hei.*

HONORS AND AWARDS

- 2025 Louisiana Impact Award, University of Louisiana at Lafayette
- 2019–2024 Academic Excellence Awards, University of Louisiana at Lafayette
- 2015 SYSU–CMU Joint Institute of Engineering Double-Degree Scholarship

SUCCEEDED GRANT EXPERIENCE

- **SaTC 2.0: RES:** The Emotional–Expert–Ethics (E^3) Framework toward Human-Centered AI Assistant Safety. *Submitted.* **Role: Co-PI.** Preliminary project link: https://mhdash.socialshields.org/.
- **RII: Track-2 FEC:** Precise Regional Forecasting via Intelligent and Rapid Harnessing of National-Scale Hydrometeorological Big Data. Total amount: $5,000,000. **NSF OIA-2019511. Role: Research Assistant.** Ranked first among student participants. Project link: https://prefer-nsf.org/.
- **CNS: CAREER:** A Holistic Framework for Constructing Dynamic Malicious Knowledge Bases in Social Networks. Total amount: $500,000. **NSF CNS-2146447. Role: Research Assistant.** Contributed to system design and technical implementation.
- **CRII: SaTC:** Empowering Elastic Honeypots as Real-Time Malicious Content Sniffers for Social Networks. Total funding: $175,000. **NSF CNS-1948374. Role: Research Assistant.** Contributed to system design and technical implementation.

PEER-REVIEWED PUBLICATIONS

CONFERENCE

20. [Submitted to ACL 25] **Y. Zhang**, S. Paul, K. Han, X. Hei . "Breach and Attack Simulation as a Lens: Exploring Misinformation in Large Language Models." *Submitted to ACL*, 2025.
19. [Submitted to NDSS 25] X. Zhang, Y. Tu, H. Kim, **Y. Zhang**, F. Hu, K. Butler, and X. Hei. "You Lock but I Flip: Exploration of An Unauthenticated Vehicle Entry via Non-Intrusive Tailgate Manipulation." *Submitted to NDSS*, 2025.
18. [Submitted to WACV 25] L. Shan, Y. Liao, K. Han, **Y. Zhang**, J. Zhang, M. I. Hossen, X. Hei . "Dynamic Attention-Guided Kernel Correction for Blind Rock CT Super-Resolution." *Submitted to WACV*, 2025.
17. [arXiv 25] M. Uddin, **Y. Zhang**, and X. Hei. "Deep Learning Aided Software Vulnerability Detection: A Survey." *Submitted to arXiv*, 2025.[paper]
16. [arXiv 24] **Y. Zhang**, N. Pakka, N.-F. Tzeng. "Knowledge Bases in Support of Large Language Models for Processing Web News." *Submitted to arXiv*, 2024.[paper]
15. **[ACM SIGKDD 24]** F. Lin, K. Guillot, S. Crawford, **Y. Zhang**, X. Yuan, and N.-F. Tzeng. "An Open and Large-Scale Dataset for Multi-Modal Climate Change-aware Crop Yield Predictions." *30th ACM SIGKDD Conference on Knowledge Discovery and Data Mining*, 2024.[paper]
14. **[ECML-PKDD 23]** F. Lin, X. Yuan, **Y. Zhang**, P. Sigdel, L. Chen, L. Peng, and N.-F. Tzeng. "Comprehensive transformer-based model architecture for real-world storm prediction." *Joint European Conference on Machine Learning and Knowledge Discovery in Databases*, 2023. [paper]
13. **[IEEE/IFIP DSN 23]** J. Lou, X. Zhang, **Y. Zhang**, X. Li, X. Yuan, and N. Zhang. "Devils in your apps: Vulnerabilities and user privacy exposure in mobile notification systems." *53rd Annual IEEE/IFIP International Conference on Dependable Systems and Networks*, 2023. **(Best Paper Award and Distinguished Paper Award)** [paper]
12. **[IEEE/CVF ICCV 23]** F. Lin, S. Crawford, K. Guillot, **Y. Zhang**, Y. Chen, X. Yuan, L. Chen, S. Williams, R. Minvielle, X. Xiao, D. Gholson, N. Ashwell, T. Setiyono, B. Tubana, L. Peng, M. Bayoumi, N.-F. Tzeng. "MMST-VIT: Climate change-aware crop yield prediction via multi-modal spatial-temporal vision transformer." *IEEE/CVF International Conference on Computer Vision*, 2023. [paper]
11. **[ACSAC 21]** **Y. Zhang**, X. Yuan, and N. Tzeng. "Platform-Oblivious Anti-Spam Gateway." *37th Annual Computer Security Applications Conference*, 2021. [paper]
10. **[ACM CCS 21]** **Y. Zhang**, X. Yuan, J. Li, J. Lou, L. Chen, and N.-F. Tzeng. "Reverse attack: Black-box attacks on collaborative recommendation." *ACM SIGSAC Conference on Computer and Communications Security*, 2021. [paper]
9. **[ECML-PKDD 21]** **Y. Zhang**, X. Yuan, S. K. Kimball, E. Rappin, L. Chen, P. Darby, T. Johnsten, L. Peng, B. Pitre, D. Bourrie, and N.-F. Tzeng. "Precise weather parameter predictions for target regions via neural networks." *Joint European Conference on Machine Learning and Knowledge Discovery in Databases*, 2021. [paper]
8. **[ESORICS 20]** **Y. Zhang**, J. Lou, L. Chen, X. Yuan, J. Li, T. Johnsten, and N.-F. Tzeng. "Towards poisoning the neural collaborative filtering-based recommender systems." *25th European Symposium on Research in Computer Security*, 2020. [paper]
7. **[ACM AsiaCCS 19]** **Y. Zhang**, H. Zhang, X. Yuan, and N.-F. Tzeng. "Tweetscore: Scoring tweets via social attribute relationships for twitter spammer detection." *25th European Symposium on Research in Computer Security*, 2019. [paper]
6. **[IEEE/IFIP DSN 19]** **Y. Zhang**, H. Zhang, X. Yuan, and N.-F. Tzeng. "Pseudo-honeypot: Toward efficient and scalable spam sniffer." *49th Annual IEEE/IFIP International Conference on Dependable Systems and Networks*, 2019. [paper]

5. [**ACM CODASPY 19**] **Y. Zhang**, H. Zhang, and X. Yuan. "Toward efficient spammers gathering in twitter social networks." *Ninth ACM Conference on Data and Application Security and Privacy*, 2019. [paper]

JOURNAL

4. [Major Revision] **Y. Zhang**, N. Pakka, X. Yuan, N.-F. Tzeng. "Real-time malicious content sniffers for online social networks.." *Major Revision*, 2025.
3. [**IEEE TGRS**] **Y. Zhang**, B. Turney, P. Sigdel, X. Yuan, E. Rappin, A. Lago, S. Kimball, L. Chen, P. Darby, L. Peng, S. Aygun, Y. Tu, M. H. Najafi, N.-F. Tzeng. "Regional Weather Variable Predictions by Machine Learning with Near-Surface Observational and Atmospheric Numerical Data." *IEEE Transactions on Geoscience and Remote Sensing*, 2025. [paper]
2. [**IEEE TPDS**] X. Yuan, X. Yuan, **Y. Zhang**, B. Li, and C. Wang. "Enabling encrypted boolean queries in geographically distributed databases." *IEEE Transactions on Parallel and Distributed Systems*, 2019. [paper]

DISSERTATION

1. [**Dissertation**] **Yihe Zhang**. "Framework for Machine Learning Approaches to Real-World Problems: Social Network Spam Detection and Weather Prediction." ***Committee**: Dr. Nian-Feng Tzeng (Chair), Dr. Li Chen, Dr. M. Hassan Najafi, Dr. Xu Yuan (University of Delaware), Dr. Neil Zhenqiang Gong (Duke University), and Dr. Sytske Kimball (University of South Alabama)*, 2024.

TEACHING EXPERIENCE

Summer 2021 – Summer 2022 Instructor

Summer Lecture on Machine Learning (ML): Applications and Practices, and Introduction to Meteorology

Spring 2019 – Spring 2023 Teaching Assistant & Lab Instructor

CMPS 413: Computer Communication and Networks

INFX 540: Informatics Network Infrastructure

ACADEMIC SERVICES

- Reviewed over 30 manuscripts for IEEE, Elsevier, Springer, and MDPI journals (IEEE Transactions on Dependable and Secure Computing, Journal of Social Network Analysis and Mining, Journal of Information Security and Applications, Results in Engineering, Engineering Applications of Artificial Intelligence, MethodsX, Industrial Crops and Products, Information Processing in Agriculture, Smart Agricultural Technology, etc.)
- Reviewed over 20 papers for top-tier computer science conferences (ACL 2025, EMNLP 2025, NeurIPS 2024, COLING 2024, WWW 2024)
- Student Volunteer, IEEE International Conference on Computer Communications, 2022

SCHOLARLY OUTREACH

1) Apr 2025 – Job Talk: *When Bad Data Attacks: Toward Safe and Responsible AI*, Kennesaw State University.

2) Nov 2024 – Invited Talk: *The Impact of Large Language Models on Misinformation: A Double-Edged Sword*, University of Texas at Arlington.

3) Nov 2021 – Research Colloquium: *Reverse Attack: Black-box Attacks on Collaborative Recommendation*, University of Louisiana at Lafayette.

4) Jul 2021 – Louisiana EPSCoR Research Report: *Precise Weather Forecasting via Intelligent and Rapid Harnessing of Big Data.*