

He Cheng

Postdoctoral Researcher, Department of Biomedical Informatics
University of Colorado Anschutz Medical Campus

📍 Aurora, CO ✉ chenghe0618@outlook.com ☎ +1 (607) 304-0392

🌐 [Personal Website](#) in [LinkedIn](#) 📄 [GitHub](#)

Research Interests

I am a **machine learning researcher** working on **large language models (LLMs)**, **knowledge graphs (KGs)**, **multi-agent systems**, and **trustworthy AI**. My current research focuses on scalable retrieval over large biomedical knowledge graphs and reinforcement learning for multi-agent clinical reasoning. My previous research focused on interpretable and robust anomaly detection, including local, global, counterfactual, and prototype-based explanations, as well as backdoor attacks against anomaly detection models. More broadly, I am interested in developing reliable, interpretable, and efficient machine learning methods for biomedical and other high-impact applications.

Education

- | | |
|---|----------------------------|
| Utah State University
<i>Ph.D. in Computer Science</i> <ul style="list-style-type: none">◦ Advisor: Dr. Shuhan Yuan◦ Dissertation: Interpretable and Robust Deep Anomaly Detection | <i>Aug 2020 - Dec 2024</i> |
| State University of New York at Binghamton
<i>M.S. in Electrical and Computer Engineering</i> <ul style="list-style-type: none">◦ Advisor: Dr. Jian Li◦ Thesis: Consensus-Based Quickest Change Detection in IoT Systems | <i>Aug 2018 - May 2020</i> |
| China University of Petroleum (East China)
<i>B.E. in Mechanical Engineering</i> | <i>Sep 2012 - Jun 2016</i> |

Publications

- [1] **He Cheng**, Yifu Wu, Saksham Khatwani, Maya Kruse, Dmitriy Dligach, Timothy A. Miller, Majid Afshar, and Yanjun Gao. "LogosKG: Hardware-Optimized Scalable and Interpretable Knowledge Graph Retrieval." *Proceedings of the 64th Annual Meeting of the Association for Computational Linguistics (ACL)*, 2026.
- [2] **He Cheng**, Depeng Xu, and Shuhan Yuan. "BadSAD: Clean-Label Backdoor Attacks against Deep Semi-Supervised Anomaly Detection." *Proceedings of the IEEE International Conference on Big Data (Big Data)*, 2025.
- [3] **He Cheng**, Depeng Xu, and Shuhan Yuan. "Backdoor Attack against Log Anomaly Detection Models." *Companion Proceedings of the 2025 ACM Web Conference (WWW)*, 2025.
- [4] **He Cheng**, Depeng Xu, Shuhan Yuan, and Xintao Wu. "Achieving Counterfactual Explanation for Sequence Anomaly Detection." *Proceedings of the European Conference on Machine Learning and Principles and Practice of Knowledge Discovery in Databases (ECML PKDD)*, 2024.
- [5] **He Cheng** and Shuhan Yuan. "Backdoor Attack against One-Class Sequential Anomaly Detection Models." *Proceedings of the Pacific-Asia Conference on Knowledge Discovery and Data Mining (PAKDD)*, 2024.
- [6] **He Cheng**, Depeng Xu, and Shuhan Yuan. "Explainable Sequential Anomaly Detection via Prototypes." *Proceedings of the International Joint Conference on Neural Networks (IJCNN)*, 2023.
- [7] **He Cheng**, Depeng Xu, and Shuhan Yuan. "Sequential Anomaly Detection with Local and Global Explanations." *Proceedings of the IEEE International Conference on Big Data (Big Data)*, 2022.
- [8] Xiao Han, **He Cheng**, Depeng Xu, and Shuhan Yuan. "InterpretableSAD: Interpretable Anomaly Detection in Sequential Log Data." *Proceedings of the IEEE International Conference on Big Data (Big Data)*, 2021.

Research Projects

Orchestrator-Centered Multi-Agent Systems for Clinical Reasoning

Jan 2026 - Present

- Developing a multi-agent system in which specialized LLM agents generate, review, and refine clinical predictions through structured multi-step interactions.
- Investigating reinforcement learning methods for training the orchestrator to select agents, assign roles, and determine when to stop based on diagnostic performance and inference cost.

Efficient and Scalable Biomedical Knowledge Graph Retrieval and LLM Integration

Jul 2025 - Jan 2026

- Designed efficient and scalable algorithms for multi-hop retrieval over large biomedical knowledge graphs (UMLS, PubMed KG), using matrix-based representations and GPU acceleration to support billion-edge graphs.
- Developed frameworks that **integrate knowledge graph retrieval with LLMs**, enabling evidence-grounded responses and improving reliability in biomedical tasks such as clinical diagnosis verification and decision support.

Backdoor Attacks Against Deep Log Anomaly Detection Models

Sep 2023 - Jun 2025

- Proposed BadSAD, a clean-label backdoor attack against Deep Semi-Supervised Anomaly Detection (DeepSAD) models, widely used for image anomaly detection. The attack involves trigger injection (embedding subtle triggers in normal images) and latent space poisoning (manipulating feature representations to misclassify triggered anomalies as normal). (*IEEE Big Data 2025*)
- Developed a backdoor attack framework for self-supervised log anomaly detection models (DeepLog, LogBERT), enabling abnormal logs to evade detection while maintaining benign performance. The attack involves data poisoning (injecting imperceptible triggers using only normal log entries) and model infection (modifying the training objective to embed the backdoor). (*WWW 2025*)
- Developed a backdoor attack framework for one-class sequential anomaly detection models (Deep SVDD, OC4Seq), enabling anomalies to evade detection while maintaining benign performance. Designed an attack strategy with trigger generation and backdoor injection. (*PAKDD 2024*)

Developing Inherently Interpretable Deep Anomaly Detection Models

Jan 2022 - Aug 2023

- Proposed a prototype-based framework for explainable sequential anomaly detection, addressing the lack of interpretability in deep learning models. The method derives multiple prototypes to represent different normal and abnormal sequence patterns, enabling instance-based explanations. It employs contrastive learning and k-means clustering to identify and explain anomalies. (*IJCNN 2023*)
- Proposed GLEAD, a globally and locally explainable anomaly detection method for sequential anomaly detection. GLEAD leverages multi-head self-attention to capture diverse anomaly patterns and derives prototypes for normal and abnormal sequences to enhance explainability. It provides local explanations by highlighting anomalous entries in sequences and global explanations by identifying common anomaly patterns across data. (*IEEE Big Data 2022*)

Explaining One-Class Deep Anomaly Detection Models via Counterfactual Explanations

Aug 2020 - Dec 2021

- Developed CFDet, a counterfactual explanation framework for one-class sequence anomaly detection (Deep SVDD, OC4Seq), identifying anomalous entries by determining the minimum changes needed to make a sequence normal. CFDet enhances interpretability in anomaly detection models, aiding security analysis and reducing false alarms. (*ECML PKDD 2024*)

Consensus-Based Quickest Change Detection in IoT Systems

Aug 2019 - May 2020

- Developed a distributed anomaly detection framework for IoT systems, enabling quickest change detection while minimizing false alarms and communication overhead. Proposed a consensus-based distributed S-CuSum algorithm, achieving performance comparable to centralized methods with reduced information exchange. Designed two optimized variants to further decrease communication costs while maintaining detection accuracy.

Research & Professional Experience

Postdoctoral Researcher

Department of Biomedical Informatics, University of Colorado Anschutz

Aurora, CO

Jul 2025 - Present

- **Knowledge Graphs and LLMs:** Developing scalable methods for multi-hop retrieval over large biomedical

knowledge graphs and integrating retrieved evidence with LLMs for clinical applications.

- **Multi-Agent Clinical Reasoning:** Developing orchestrator-centered multi-agent systems in which specialized LLM agents generate, review, and refine clinical predictions, with reinforcement learning methods for agent selection, role assignment, and stopping decisions.
- **Collaboration:** Working with clinicians and researchers to develop LLM-based systems aligned with diagnostic and clinical decision-support workflows.

Volunteer Research Assistant

Utah State University

Logan, UT

Jan 2025 - Jun 2025

- **Research:** Collaborated with Dr. Shuhan Yuan as a volunteer researcher to finalize academic publications and extend experimental evaluations of deep anomaly detection models.

Research Assistant

Utah State University

Logan, UT

Aug 2020 - Dec 2024

- **End-to-End Machine Learning Systems:** Designed and implemented machine learning pipelines for log anomaly detection using **PyTorch** and **TensorFlow**. Developed **counterfactual explanations**, **global and local interpretability**, and **prototype-based insights** to enhance user trust and identify vulnerabilities in deep anomaly detection systems.
- **Linux Server Management:** Configured SSH access for new users and managed distributed servers for machine learning experiments. Automated routine system monitoring using Bash scripts and analyzed logs and resource usage to improve GPU utilization and experiment reliability.

Teaching & Mentorship

Teaching Assistant

Department of Computer Science, Utah State University

Logan, UT

Aug 2021 - Dec 2024

- Assisted in teaching and grading coursework for the following courses:
 - CS 5665 Introduction to Data Science
 - CS 5080/CS 6665 Data Mining

Academic Service

Reviewer, ACM Transactions on Intelligent Systems and Technology (TIST)	2026
Reviewer, ACL Rolling Review (ARR)	2026
Reviewer, International Joint Conference on Neural Networks (IJCNN)	2025
Reviewer, Pacific-Asia Conference on Knowledge Discovery and Data Mining (PAKDD)	2025
Reviewer, International Conference on Machine Learning and Applications (ICMLA)	2024
Reviewer, International Joint Conference on Neural Networks (IJCNN)	2024
Reviewer, International Joint Conference on Neural Networks (IJCNN)	2023
Reviewer, IEEE Transactions on Computational Social Systems	
Reviewer, Concurrency and Computation: Practice and Experience	
Reviewer, Intelligent Data Analysis	

Awards

Volunteer Lead, IEEE International Conference on Big Data	2024
SDM'24 Doctoral Forum Travel Award (\$1,000)	2024
Utah State University Graduate Student Travel Award	2023
Utah State University Graduate Student Travel Award	2022

Technical Skills

Programming and Systems: Python, SQL, C/C++, Bash, Linux, Git, Docker

Machine Learning and LLM Frameworks: PyTorch, TensorFlow, Hugging Face Transformers, PEFT/LoRA, LangChain, LangGraph, FastMCP, SGLang

Research Areas and Methods: Large Language Models, Knowledge Graphs, Multi-Agent Systems, Reinforcement Learning, Retrieval-Augmented Generation, Interpretable AI, Robust Machine Learning, Anomaly Detection

Cloud and Databases: AWS, GCP, PostgreSQL, MongoDB, SQLite, Neo4j