YUE ZHANG

Ph.D. Student | Computer Science & Software Engineering

zyue110026@outlook.com +1 (334) 752-9292 662 Spring Street, Auburn, AL 36830 USA
yue-zhang-1592b0236 zyue110026 https://zyue110026.github.io/ 0000-0001-7421-7833

EDUCATION

Doctor of Science in Computer Science & Software Engineering

Auburn University

08/2023 – 04/2027

GPA: 3.86 / 4.0

AWARDS

- **100+ Women Strong Outstanding Departmental Annual Graduate Award**, Auburn University *03/2024*
- **2023 Gavin Graduate Student Fellow**, Auburn University *04/2023*
- **Second-class Scholarship** (Top 5%), Anhui Jianzhu University *11/2019*
- **Excellent Minister of Student Union**, Anhui Jianzhu University *10/2019*
- **Third-Class Scholarship** (Top 10%), Anhui Jianzhu University *11/2018*

OPEN SOURCE CONTRIBUTIONS

- Discovered and reported 19 previously unknown bugs across 15 Kubernetes GitHub repositories using static analysis, all confirmed and fixed by maintainers. [1], [2], [3], [4], [5], [6], [7], [8], [9], [10], [11], [12], [13], [14], [15]
- Identified and Reported 2 security-related issues involving Kubernetes pod configuration parameters across 2 GitHub repositories using t-way covering; both were fixed. [1], [2]

SKILLS

- **Programming Languages**: Python, R, JavaScript, SQL
- **Web Development**: ReactJS, Flutter
- **Tools & Frameworks**: WEKA, ChatGPT-4o, DeepSeek-R1, Llama-3.1
- **Database Management**: SQL, Firebase
- **Machine Learning & Data Analytics**: Data modeling, Data visualization
- **Cloud Management**: Kubernetes

PUBLICATIONS

1. **Yue Zhang**, Ucchwas Paul, Marcelo d' Amorim, and Akond Rahman (2026), Configuration Defects in Kubernetes, *IEEE Transactions on Software Engineering (TSE), 2026.*
2. Jiawei Tyler Gu, Zhen Tang, Yiming Su, Bogdan Alexandru Stoica, Xudong Sun, William X. Zheng, **Yue Zhang**, Akond Rahman, Chen Wang, and Tianyin Xu (2025), Who Watches the Watchers? On the Reliability of Softwarizing Cloud Application Management, *Networked Systems Design and Implementation (NSDI '26 Spring Artifact Evaluation).*
3. Akond Rahman, Gerry Dozier, and **Yue Zhang**, (2025), Authorship of Minor Contributors in Kubernetes Configuration Scripts: An Exploratory Study, *Causal Methods in Software Engineering (CauSE 2025).*
4. **Yue Zhang**, Justin Murphy, and Akond Rahman, (2025), *Come for Syntax, Stay for Speed, Write Secure Code*: An Empirical Study of Security Weaknesses in Julia Programs, *Empirical Software Engineering Journal (EMSE).*
5. Akond Rahman, Anthony Skjellum, and **Yue Zhang**, (2025), An Exploratory Study of Security Vulnerabilities in Machine, *3rd International Workshop on Software Vulnerability Management (SVM 2025).*
6. Pemsith Mendis, Wilson Reeves, Muhammad Ali Babar, **Yue Zhang**, and Akond Rahman, (2024), Evaluating the Quality of Open Source Ansible Playbooks: An Executability Perspective, *4th International Workshop on Software Engineering and AI for Data Quality in Cyber-Physical Systems/Internet of Things (SEA4DQ 2024) co-located with the Foundations of Software Engineering (FSE).*
7. Akond Rahman, **Yue Zhang**, Fan Wu, and Hossain Shahriar, (2024), Student Perceptions of Authentic Learning to Learn White-box Testing, *Technical Symposium on Computer Science Education (SIGCSE TS).*

8. **Yue Zhang**, Rachel Meredith, Wilson Reeves, Julia Coriolano, Ali Babar, and Akond Rahman, (2024), Does Generative AI Generate Smells Related to Container Orchestration?: An Exploratory Study with Kubernetes Manifests, *21st International Conference on Mining Software Repositories 2024*
9. Akond Rahman, Dibyendu Brinto Bose, **Yue Zhang**, and Rahul Pandita, (2024), An Empirical Study of Task Infections in Ansible Scripts, *Empirical Software Engineering Journal*.
10. **Yue Zhang,** Muktadir Rahman, Fan Wu and Akond Rahman, (2023), Quality Assurance for Infrastructure Orchestrators: Emerging Results from Ansible, *2nd International Workshop on the Foundations of Infrastructure Specification and Testing (FIST 2023), L'Aquila, Italy, March 13th 2023*.
11. **Yue Zhang,** Fan Wu and Akond Rahman, (2023), Practitioner Perceptions of Ansible Test Smells, *2nd International Workshop on the Foundations of Infrastructure Specification and Testing (FIST 2023), L'Aquila, Italy, March 13th 2023*.

RESEARCH PROJECTS

Individual or Combinatorial?: Configuration Parameters of Kubernetes Pods that Facilitate Security Attacks

Auburn University

08/2024 – 07/2025

Adviser: Dr. Akond Ashfaque Ur Rahman
Graduate research assistantship supported by NSF under Award numbers #2247141 and #2312321.

- Conducted an empirical study using the MITRE ATT&CK framework to identify Kubernetes pod configuration parameters enabling 7 security attacks, evaluated detection techniques including t-way covering arrays, large language models, and SAST tools, and provided recommendations to mitigate these attacks.
- Identified and reported 12 combinations of Kubernetes pod configuration parameters that facilitate security attacks; 2 reports were accepted, and 1 has been fixed.
- Technologies: Empirical analysis, Kubernetes security, static analysis, large language models.

Configuration Bugs in Kubernetes

Auburn University

08/2023 – 07/2024

Adviser: Dr. Akond Ashfaque Ur Rahman
Graduate research assistantship supported by NSF under Award numbers #2247141 and #2312321.

- Investigated configuration defects in Kubernetes to enhance system reliability and security. Designed and developed an automated tool to detect misconfigurations in Kubernetes YAML files, aiming to reduce deployment failures and minimize security risks.
- Found and reported 44 configuration-related bugs in Kubernetes YAML files; 26 were accepted, and 19 have been fixed, contributing to improved deployment reliability and security.
- Technologies: Static analysis, Kubernetes, Python.

Come for Syntax, Stay for Speed, Write Secure Code: An Empirical Study of Security Weaknesses in Julia Programs

Auburn University

07/2023 – 09/2023

Adviser: Dr. Akond Ashfaque Ur Rahman
Graduate research assistantship supported by NSF under Award numbers #2247141, #2310179, #2312321, and NSA Award #H98230-21-1-0175.

- Conducting an empirical study to systematically identify and characterize security weaknesses in Julia programs, which are widely used in data science, scientific computing, and machine learning.
- Aimed at facilitating secure development of Julia-based scientific software by analyzing patterns and causes of security issues in real-world codebases.
- Technologies: Julia, static analysis, empirical software engineering.