Shazibul Islam Shamim

mzs0283@auburn.edu • +1 (931) 252-8439 • https://shazibulislam.github.io • https://github.com/shazibulislam/

EDUCATION

Auburn University, Auburn, AL, USA — Aug 2022 - May 2024 (Expected)

- Ph.D. in Computer Science
  - Research areas: Software Engineering, Secure Software Engineering, DevOps.
  - Adviser: Dr. Akond Rahman

Tennessee Tech University, Cookeville, TN, USA — Jan 2020 - Aug 2022

- Ph.D. in Computer Science (Transferred to Auburn University)
  - Adviser: Dr. Akond Rahman

Bangladesh University of Engineering & Technology (BUET), Dhaka, Bangladesh — Feb 2011 - Nov 2016

- B.Sc. in Computer Science & Engineering
  - Thesis: An Exact and Efficient Parallel Algorithm for Planted Motif Search
  - Adviser: Dr. Md. Abul Kashem Mia

PUBLICATIONS

[1] **Shazibul Islam Shamim**, Jonathan Alexander Gibson, Patrick Morrison, and Akond Rahman. **Benefits, Challenges, and Research Topics: A Multi-vocal Literature Review of Kubernetes**. *ACM Transactions on Software Engineering and Methodology (under review)*

[2] Akond Rahman, **Shazibul Islam Shamim**, Dibyendu Brinto Bose, and Rahul Pandita. **Security Misconfigurations in Open Source Kubernetes Manifests: An Empirical Study**. *ACM Transactions on Software Engineering and Methodology*, 32(4), May 2023

[3] **Shazibul Islam Shamim**. **Mitigating Security Attacks in Kubernetes Manifests for Security Best Practices Violation**. In *Proceedings of the 29th ACM Joint Meeting on European Software Engineering Conference and Symposium on the Foundations of Software Engineering*, ESEC/FSE 2021, page 1689–1690, New York, NY, USA, 2021. Association for Computing Machinery

[4] Dibyendu Brinto Bose, Akond Rahman, and **Shazibul Islam Shamim**. **'Under-reported' Security Defects in Kubernetes Manifests**. In *2021 IEEE/ACM 2nd International Workshop on Engineering and Cybersecurity of Critical Systems (EnCyCriS)*, pages 9–12, 2021

[5] **Shazibul Islam Shamim**, Farzana Ahamed Bhuiyan, and Akond Rahman. **XI Commandments of Kubernetes Security: A Systematization of Knowledge Related to Kubernetes Security Practices**. *Proceedings of the 2020 IEEE Secure Development Conference(SecDev), Atlanta,GA*, 2020

[6] Justin Murphy, Elias T. Brady, **Shazibul Islam Shamim**, and Akond Rahman. **A Curated Dataset of Security Defects in Scientific Software Projects**. In *Proceedings of the 7th Symposium on Hot Topics in the Science of Security*, HotSoS '20, New York, NY, USA, 2020. Association for Computing Machinery

[7] Akond Rahman, **Shazibul Islam Shamim**, Hossain Shahriar, and Fan Wu. **Can We Use Authentic Learning to Educate Students about Secure Infrastructure as Code Development?** In *Proceedings of the 27th ACM Conference on on Innovation and Technology in Computer Science Education Vol. 2*, ITiCSE '22, page 631, New York, NY, USA, 2022. Association for Computing Machinery

AWARDS

BRONZE AWARD WINNER Student Research Competition at **ACM ESEC/FSE 2021**

1ST RUNNER UP Research Poster Presentation at Bioinformatics and Stringology Conference 2015

Awarded **Travel Grant** for **ACM ESEC/FSE 2021**, Greece

CHAMPION National Software Project Show at BUET CSE Festival 2015.

RESEARCH PROJECTS

Graduate Research Assistant, PASER Group — Jan 2020 – Dec 2023

- **An automated security analysis framework for Kubernetes pod configurations**

In this project, we aim to help the practitioners to have a proper understanding of the consequences of security misconfigurations. Static analysis tools cannot ensure the soundness and completeness of the source code evaluation. Furthermore, practitioners may need to understand how a security misconfiguration can make a Kubernetes cluster vulnerable to attacks. Static analysis tools cannot generate information for potential attack scenarios or demonstrate a realizable attack path by identifying a security misconfiguration in a source code file. To help practitioners understand the implications of security misconfigurations, we combine model checking with a static analysis tool to identify known attacks on security misconfigurations in Kubernetes manifests. We have created a finite state model based on the interaction of pod life cycle and container states. We extract pod properties systematically by analyzing Internet artifacts related to pod requirements. We use a model checker, NuXmv, to validate 10 pod security requirements constructed from OWASP's top 10 vulnerabilities, verify 6 action sequences, and determine attack-akin configurations that lead to an attack. We have extended our open-source static analysis tool, SLIKUBE, to create a new static analysis tool called SLIKUBE+. This tool helps us identify 23 attack-akin security misconfigurations in Kubernetes.**[Paper in progress]**

RESEARCH PROJECTS

- **Quantifying the Efficacy of Security Analysis Tools for Kubernetes**

Industry practitioners follow security guidelines such as CIS benchmarks to secure Kubernetes-based deployments. In our collaborative research with Wind River, we discovered that no individual security analysis tool offers comprehensive coverage for the AWS CIS benchmark. Our survey of industry practitioners has revealed that practitioners have diverse opinions on security recommendations associated with the AWS CIS benchmark. Furthermore, we observed that security analysis tool results do not always agree with each other, as we have observed with our constructed Oracle datasets from proprietary source codes. **[Paper in progress]**

- **Authentic Learning-based Curriculum for Kubernetes Security Misconfiguration Analysis**

In this project, we created an authentic learning-based exercises to help the students understand Kubernetes security misconfigurations. As a part of the authentic learning exercise, we designed hands-on and post-lab exercises in real-world scenarios and the necessary background for the exercise as pre-lab content. In the Fall 22 and Spring 23 semesters, we deployed our designed curriculum in software engineering and security-related courses at Auburn University and Tuskegee University, respectively, and received 127 student responses. From the responses, 92.6% of students reported that all three exercise steps were helpful. Also, 87.4% of students say authentic learning-based exercises helped them learn about Kubernetes misconfigurations. **[Paper in progress]**

- **Mitigating attacks on Kubernetes cluster for security best practices violations**

In this project, I have tried to exploit a minimal Kubernetes cluster for security best practices violations and also proposed potential mitigation strategies. I submitted my initial idea and results to the ACM student research competition in **ESEC/FSE 2021** and won the Bronze award in the Graduate category.

- **Multi-vocal Literature review on Kubernetes**

We systematically curated and performed qualitative analysis on **105 academic publications** and **321 Internet artifacts** such as blog posts, videos, and presentations related to Kubernetes. We identified eight benefits such as **'Ease in Cloud-based Interfacing', 'Community Support'** and 15 challenges such as **'Cultural Change', 'Learning Curve'** as described by the practitioners and 14 research areas in Kubernetes from academic publications. This work is currently under review.

- **Identifying the violation of security practices in OSS projects related to Kubernetes**

We conducted a grey literature review on **104 Internet artifacts** such as blog posts, videos and presentations related to Kubernetes security practices. We synthesized a list of **11 security practices** and built a curated dataset with a mapping between Internet artifacts and identified security practices. The paper was accepted in **IEEE SecDev 2020**, a peer-reviewed conference in Secure Software Development. We have conducted **qualitative analysis on open source Kubernetes** repositories and built a **static analysis tool with taint tracking** for tracking the flow of information in Kubernetes cluster for automatically identifying violation of security practices in Kubernetes manifests. This work is published in **ACM Transactions on Software Engineering and Methodology (TOSEM)**.

Undergraduate Thesis, Bangladesh University of Engineering and Technology — Mar 2015 – Feb 2016

- **Designing parallel algorithms for planted motif search**

I reproduced and generated the results of *qPMS9, PMS8, qPMS7* algorithms and proposed a new parallel algorithm *PMS-Alpha* for planted motif search. Implemented and compared the results with *qPMS9, PMS8 with PMS-Alpha* for performance benchmarks. Additionally, I submitted my final result as a Poster to Bioinformatics and Stringology Conference **BIOS '15** in BUET, Dhaka, and received the **1st Runner Up** award.

INVITED TALKS

- **"Towards Building a Reliable Kubernetes Security Analysis Ecosystem"**, Invited Research Talk, WindRiver Associates at WindRiver September Technical Symposium on September 13, 2023
- **"Mitigating Security Attacks in Kubernetes Cluster"**, Invited Research Talk at National Security Agency CAE Forum Talks for Cybersecurity Community on December 1, 2021 Link

PROFESSIONAL EXPERIENCE

Graduate Teaching Assistant, Auburn University — Jan 2024 – Present

As a teaching assistant for **COMP 3270: Introduction to Algorithms**, I conduct lectures on behalf of the course instructor, Dr. Levent Yilmaz. I assist students with in-lecture activities, grade their work, and help during office hours. Moreover, I also conduct on-demand recitation sessions to help students understand theoretical concepts.

DevSecOps Research Intern, Wind River Systems, USA (Remote) — May 2023 – Aug 2023

Mentor: Hanyang Hu, Karen Smiley

- Created a map between AWS CIS Kubernetes recommendations and the rules of open-source Kubernetes security analysis tools.
- Designed and conducted a survey among the practitioners to understand their perceptions of Kubernetes CIS recommendations.
- Created an Oracle dataset from the proprietary repositories and executed static analysis tools on the Oracle dataset.
- Reported precision, recall and low agreements, coverage among the static analysis tools on the static analysis results.
- Collaborated with the product security team to execute dynamic analysis tools in production clusters and reported low AWS CIS Kubernetes recommendation coverage and low agreement among the dynamic analysis tool.

Data Science Intern, GEODIS, Brentwood,TN, USA (Remote) — May 2022 – Aug 2022

Mentor: Dr. Seratun Jannat

- Collaborated with the data team and internal stakeholders to identify 66 relevant attributes out of 780 in the data of the past 24 months.
- Performed feature selection on the relevant attributes and identified 15 attributes that are correlated more with the freight inspection.
- Conducted statistical analysis and created visualizations to explore freight inspection, which is a rare event ($<0.02\%$).
- Developed several machine learning models for freight inspection prediction, and proposed an autoencoder model that outperformed other models by uncovering latent patterns in the data related to freight inspection.

PROFESSIONAL EXPERIENCE

Software Engineer (DevOps), iPay Systems Limited., Dhaka, Bangladesh Sep 2016 – Dec 2019
Team Lead: Minhaj Ahamed Abir

- Increased deployment frequency by **200%** and reduced downtime by automating CI/CD pipelines with Jenkins, Ansible, and deploying Docker containers in production Docker swarm cluster.
- Configured and managed the ELK cluster for a centralized logging system with Apache Kafka and Zookeeper.
- Built real-time monitoring and alert systems for the Kibana visualizer and Elastic search for the production application.
- Performed security scanning for vulnerabilities in the production cluster to comply with **PCI-DSS** standards.
- Developed a cross-platform automated test suite for mobile platforms such as Android, iOS and web platforms with Calabash, Appium, and Capybara frameworks, respectively, that **saved 20 hours for UI feature testing time for each release.**
- Designed API automated test suites and used SonarQube for code security analysis with CI pipeline that **saved 10 hours per release**.

SKILLS

Programming: Python, Java, C, C++, Bash, HTML, CSS

Web & DB: MySQL, PostgreSQL, AWS, Google Cloud Platform, Azure.

Libraries: Numpy, Pandas, NLTK, Spacy, Pandas, Scikit-Learn, Tensorflow, Keras

Tool: Docker, LaTeX, Git, Jenkins, Docker, Kubernetes, Apache Kafka, Elastic search, Logstash, Kibana.

EXTRA CURRICULAR ACTIVITIES

President, Computer Science Graduate Club, Tennessee Tech University Aug 2021 – Jul 2022
President, Bangladeshi Student Association, Tennessee Tech University Aug 2021 – Jul 2022

REFERENCE

Dr. Akond Rahman
Assistant Professor
Auburn University
Email: azr0154@auburn.edu

Dr. Seratun Jannat
Lead Data Scientist,
GEODIS
Email:seratun.jannat@geodis.com

Hanyang Hu
Team Lead, Developer Experience AI team
Wind River Systems
Email: phenom.hu@windriver.com