Md Rayhanur Rahman

mrahman87@ua.edu https://rayhanur-rahman.github.io
0000-0003-4980-7350 Google Scholar DBLP

Summary

My research interests are software security, cyberthreat intelligence, and cyberthreat hunting. My research group focuses on (a) identifying malicious packages in open-source software supply chain ecosystem, and (b) mining actionable intelligence from open-source knowledge bases for software and security practitioners to design proactive defenses. I rely on a wide range of techniques, such as natural language understanding, generative AI, machine learning, static analysis, and grounded theory-based approaches.

Education

2018 – 2024 **Ph.D. in Computer Science, North Carolina State University**
Thesis title: *Towards mining proactive intelligence from OSCTI reports*
Advisor: Dr. Laurie Williams

2013 – 2014 **M.Sc. in Software Engineering, University of Dhaka**
Thesis title: *Towards peer to peer resource provisioning in cloud*
Advisor: Dr. Kazi Muheymin-Us-Sakib

2009 – 2012 **B.IT. in Software Engineering, University of Dhaka**

Work Experience

2024 – · · · · **Assistant Professor** at the University of Alabama at Tuscaloosa
I have been a tenure track assistant professor since August 2024 with a primary research focus on software security, cyberthreat intelligence, and machine learning.

2020 – 2020 **Research Intern** at Microsoft Corporation
I have worked with 1ES team to analyze and investigate how the security tools can be improved through empirical methods.

2018 – 2024 **Graduate Assistant** at North Carolina State University
I served as a research assistant as part of NSA Science of Security Lablet. I investigate the open-source technical reports of past cyberattack incidents to mine malicious behavior patterns. I leverage the patterns to provide proactive and actionable insights for security practitioners. I also served as a teaching assistant for four semesters in software engineering, software security, and DevOps-related courses.

2021 – 2021 **Summer Teaching Instructor** at North Carolina State University
I have worked as a summer teaching instructor for C and Software Tools courses designed for undergraduate students.

2014 – 2018 **Lecturer** at University of Dhaka
I taught undergraduate courses such as Discrete Mathematics, Data Structure, Combinatorial Optimization, Object Oriented Concepts, and Operating Systems. I also taught Formal Methods and Models of Software Engineering to graduate students. Apart from teaching, I oversaw undergraduate students' academic affairs and designed course curricula for external institutions.

2015 – 2017 **Guest Lecturer** at Daffodil International University, Dhaka
I taught undergraduate courses: Software Engineering and Object-oriented Concepts.

2015 – 2016 **Guest Lecturer** at East West University, Dhaka
I taught undergraduate courses: Introduction to Computing.

2013 – 2014 **Junior Software Engineer** at Kaz Software
I worked on a proprietary Google Chrome extension named LinkableNews and a web application named LinkableService, which provided web ontology and identity services.

Selected Research Publications

Journal Articles (Published)

1. S. Elder, **Md Rayhanur Rahman**, G. finger, K. Kapoor, and L. Williams, "A survey on software vulnerability exploitability assessment," *ACM Computing Survey*, 2024.
2. **Md Rayhanur Rahman**, R. Mahdavi-Hezaveh, and L. Williams, "What are the attackers doing now? automating cyberthreat intelligence extraction from text on pace with the changing threat landscape: A survey," *ACM Computing Surveys*, vol. 55, no. 12, pp. 1–36, 2023.
3. **Md Rayhanur Rahman**, N. Imtiaz, M.-A. Storey, and L. Williams, "Why secret detection tools are not enough: It's not just about false positives-an industrial case study," *Empirical Software Engineering*, vol. 27, no. 3, p. 59, 2022.
4. A. Rahman, **Md Rayhanur Rahman**, C. Parnin, and L. Williams, "Security smells in ansible and chef scripts: A replication study," *ACM Transactions on Software Engineering and Methodology (TOSEM)*, vol. 30, no. 1, pp. 1–31, 2021.
5. M. M. Rahman, R. R. Riyadh, S. M. Khaled, A. Satter, and **Md Rayhanur Rahman**, "Mmruc3: A recommendation approach of move method refactoring using coupling, cohesion, and contextual similarity to enhance software design," *Software: Practice and Experience*, vol. 48, no. 9, pp. 1560–1587, 2018.
6. **Md Rayhanur Rahman** and K. Sakib, "A scalable resource provisioning scheme for the cloud using peer to peer resource discovery and multi-attribute utility theory," *International Journal of Cloud Computing*, vol. 6, no. 3, pp. 211–237, 2017.
7. M. M. Rahman, **Md Rayhanur Rahman**, and B. M. Hossain, "Recommendation of move method refactoring to optimize modularization using conceptual similarity," *International Journal of Information Technology and Computer Science*, 2017.
8. M. M. Rahman, S. Rahman, **Md Rayhanur Rahman**, B. M. Hossain, and M. Shoyaib, "Dtcth: A discriminative local pattern descriptor for image classification," *EURASIP Journal on Image and Video Processing*, vol. 2017, pp. 1–24, 2017.
9. A. Imran, A. U. Gias, **Md Rayhanur Rahman**, and K. Sakib, "Provintsec: A provenance cognition blueprint ensuring integrity and security for real life open source cloud," *International Journal of Information Privacy, Security and Integrity*, vol. 1, no. 4, pp. 360–380, 2013.

Conference Proceedings (Published)

1. **Md Rayhanur Rahman**, B. Wroblewski, Q. Matthews, B. Morgan, T. Menzies, and L. Williams, "Chronocti: Mining knowledge graph of temporal relations among cyberattack actions," in *IEEE International Conference on Data Mining*, 2024.
2. **Md Rayhanur Rahman**, B. Wroblewski, M. Tamanna, I. Rahman, A. Anufryienak, and L. Williams, "Towards a taxonomy of challenges in security control implementation," in *2024 Annual Computer Security Application Conference*, IEEE, 2024.
3. **Md Rayhanur Rahman**, W. Enck, and L. Williams, "Do configuration management tools make systems more secure? an empirical research plan," in *Proceedings of the 7th Symposium on Hot Topics in the Science of Security*, 2020, pp. 1–2.
4. **Md Rayhanur Rahman**, R. Mahdavi-Hezaveh, and L. Williams, "A literature review on mining cyberthreat intelligence from unstructured texts," in *2020 International Conference on Data Mining Workshops (ICDMW)*, IEEE, 2020, pp. 516–525.
5. **Md Rayhanur Rahman**, A. Rahman, and L. Williams, "Share, but be aware: Security smells in python gists," in *2019 IEEE International conference on software maintenance and evolution (ICSME)*, IEEE, 2019, pp. 536–540.
6. A. S. Ami, M. M. Hasan, **Md Rayhanur Rahman**, and K. Sakib, "Mobicomonkey: Context testing of android apps," in *Proceedings of the 5th International Conference on Mobile Software Engineering and Systems*, 2018, pp. 76–79.

In Review

1. **Md Rayhanur Rahman**, R. Mahdavi-Hezaveh, S. Basak, and L. Williams, "Attackers reveal their arsenal: An investigation of adversarial techniques in cti reports," *ACM Transactions on Software Engineering and Methodology*, 2024.
2. **Md Rayhanur Rahman**, I. Rahman, and L. Williams, "If you cannot measure it, you cannot secure it. a case study on metrics for informed choice of security controls," *Journal of Information Security and Applications*, 2024.

Preprints

1. **Md Rayhanur Rahman** and L. Williams, "An investigation of security controls and mitre att\&ck techniques," *arXiv preprint arXiv:2211.06500*, 2022.
2. **Md Rayhanur Rahman** and L. Williams, "From threat reports to continuous threat intelligence: A comparison of attack technique extraction methods from textual artifacts," *arXiv preprint arXiv:2210.02601*, 2022.
3. **Md Rayhanur Rahman** and L. Williams, "Investigating co-occurrences of mitre att\&ck techniques," *arXiv preprint arXiv:2211.06495*, 2022.

Skills

Research methods	Mixed methods, meta-analysis, grounded theory approach, survey, empirical analysis
Machine learning	Classical learning, deep learning, graph learning, multi-modal learning, association rule mining, social network analysis
Natural language processing	Transformers, large language models, language representation learning, fine-tuning, semantic analysis, text classification, entity and relation extraction, knowledge graph extraction
Cybersecurity	Threat intelligence, security control, threat modelling, MITRE ATT&CK, NVD, CWE, NIST SP800-53, vulnerability analysis
Program Analysis	Static analysis, abstract syntax tree
Tools	PyTorch, Deep graph library, Scikit-learn, Networkx, Spacy, OpenAI, Transformers, CodeQL, ZAP, Fortify
Languages	Python, C#, Javascript, Prolog, Java, C

Research Tools

ChronoCTI	Extracting temporal patterns of malicious malware behavior from open source textual descriptions of past cyberattacks
PyGistSecuritySmell	A static analyzer for finding security weaknesses in Python
SLIC-Ansible	A static analyzer for finding security weaknesses in Ansible scripts
Scalable-VFDT	An online tree based learner for software defect predictions for large-scale codebases

Miscellaneous

Scholarly Contribution

2025	**Program Committee member** at the International Conference on Software Engineering (ICSE) 2026
	Program Committee member at the International Conference on Evaluation and Assessment in Software Engineering (EASE) 2025
2024	**Reviewer** for Scientific Reports, Springer
	Reviewer for Journal of System and Software, Springer
	Guest Talk Large Language Models and Secure Coding, NC State University
	Reviewer for Heliyon
2023	**Reviewer** for Computers & Security
	Guest Talk Inviting Security and Privacy into DevOps, NC State University
2021	**Sub-reviewer** for International Conference of Software Engineering
	Sub-reviewer for International Conference of Software Engineering
2020	**Sub-reviewer** for Mining Software Repositories
	Sub-reviewer for Empirical Software Engineering Methods, and Measurements

Miscellaneous (continued)

Teaching

- 2024 — **CS691-002: Software Supply Chain Security**: The University of Alabama
- 2014-2018 — **Undergraduate courses:** Discrete Mathematics, Object-oriented Concepts, Combinatorial Optimization, Operating System and System Programming, Distributed Systems, Computer Data and Network Security, Introduction to Computing
- **Graduate courses:** Formal Methods and Models in Software Engineering, Distributed Software Engineering
- 2021 — **Undergraduate courses:** C and Software Tools
- 2018-2024 — **Teaching Assistant:** Software Engineering, DevOps, Software Security

Mentoring

- 2025 — **PhD Student**: Md Nazmul Hoque
- 2024 — **Undergraduate students**: Brandon Wroblewski, Andrew Anufryienak
- 2023 — **Undergraduate students**: Brantley Morgan, Brandon Wroblewski, Quinn Matthews
- 2022 — **Undergraduate students**: Jonathan Buck
- 2021 — **Graduate students**: Aishwarya Seth
- 2017 — **Graduate Students**: Deepak Chandra Das
- 2016 — **Graduate Students**: Masudur Rahman
- 2015 — **Graduate Students**: Md Shafiuzzaman

Awards and Achievements

- 2025 — **Hewson College of Engineering Fellow** - The University of Alabama
- 2024 — **Mentored Teaching Fellowship - Software Security**, College of Engineering, NC State University
- 2020 — **Travel Grant**, Science of Security, National Security Agency
- 2019 — **Travel Grant**, College of Engineering, NC State University, United States
- 2017 — **Research Grant**, United Grants Commission, Bangladesh
- 2016 — **Research Grant**, United Grants Commission, Bangladesh
- 2015 — **Innovation Fund**, Ministry of Information, Communication and Technology, Government of Bangladesh
- 2014 — **National Science and Technology Fellowship**, Ministry of Science and Technology, Government of Bangladesh
- 2012 — **Champion**, ByteKnight Cybersecurity Challenge, organized by OWASP, Bangladesh
- **Finalist**, Microsoft Imagine Cup, Bangladesh
- 2011 — **Champion**, GetRoot Cybersecurity Challenge, organized by OWASP, Bangladesh

References

1. **Dr. Laurie Williams**
   Distinguished University Professor, Computer Science, NC State University
   Email: lawilli3@ncsu.edu
   Cell: 919-513-4151

2. **Dr. Munindar P. Singh**
   SAS Institute Distinguished Professor of Computer Science, Computer Science, NC State University
   Email: mpsingh@ncsu.edu
   Cell: 919-515-5677

3. **Dr. Timothy Menzies**
   Professor, Computer Science, NC State University
   Email: tjmenzie@ncsu.edu
   Cell: 304-376-2859

4. **Dr. Akond Rahman**
   Assistant Professor, Computer Science and Software Engineering, Auburn University
   Email: akond@auburn.edu
   Cell: 334-844-6352

5. **Dr. John-Paul Ore**
   Assistant Professor, Computer Science, NC State University
   Email: jwore@ncsu.edu
   Cell: 919-515-5164