Nidhi **Rastogi**

Assistant Professor, Rochester Institute of Technology, NY

(513) 417-7449 | iamnidhirastogi@gmail.com | nidhirastogi.github.io | ai4sec | nidhirastogi

Research Interests

Cyber Threat Intelligence, Machine Learning (Neural Networks & Reinforcement Learning), Data Science, Graph Analytics, Networks, Knowledge Graphs, Critical Infrastructures, Terrorism, Societal Impact of AI.

Academic Appointments

Rochester Institute of Technology

Rochester, NY

Assistant Professor (tenure-track), Department of Software Engineering — *Aug. 2021 - Present*

- Advising 3 Ph.D. Graduate students, 5 Master, and 1 Undergraduate researcher.
- Affiliate Faculty, ESL Global Cybersecurity Institute, RIT. On grant awards and recruitment committees.
- PhD Selection Committee, Golisano College of Computing and Information Sciences, 2023
- NSF review panelist.

Rensselaer Polytechnic Institute

Troy, NY

Research Scientist, IDEA Institute — *July. 2019 - Aug. 2021*

- Advised 1 Ph.D. graduate student, 2 Master, and 9 Undergraduate researchers.
- Affiliate Faculty, ESL Global Cybersecurity Institute, RIT.

Troy, NY

Postdoctoral Researcher, IDEA Institute — *Dec. 2018 - July. 2019*

- Advised 1 Ph.D. graduate student, 2 M.S., and 11 Undergraduate researchers.
- Affiliate Faculty, ESL Global Cybersecurity Institute, RIT.

Education

Rensselaer Polytechnic Institute

Troy, NY

Ph.D. in Computer Science, Advisor: Dr. James A. Hendler — *2018*

- Thesis: A Novel Security Scheme during Vertical Handoff in Integrated Heterogeneous Wireless Networks
- Finalist Graduate Student Award, FADEx laureate for 1st French-American Program on Cyber-Physical Systems, mentored 5 undergraduate and graduate students, TA for 3 courses, IBM Graduate Researcher Awrad.
- Interned at IBM Research (built centrality models to analyze real network data), GE Global Research (tested Chain-of-trust), and BBN Raytheon (designed Threat Models for tactical network)

University of Cincinnati

Cincinnati, OH

M.S. in Computer Science — *2008*

- Thesis: A Novel Security Scheme during Vertical Handoff in Integrated Heterogeneous Wireless Networks.
- Graduate Student Scholarship for entire Masters (100% tuition waiver given to top 5% applicants to the university).
- Interned at Yahoo (program start/stop remote wireless devices on Y! network) and Verizon Wireless (device security).

University of Delhi

Delhi, New Delhi

Bachelor of Information Technology — *2003*

- Second place– Annual Debate Competition, First place– Freshman of the Year award.

Grants and Contracts

Received. Total Value as PI, Co-PI,or Collaborator: $845,000

- **Autonomous agents for Cyber Protection– $80,000**, Sierra Nevada Corporation, Benjamin Blakely, Argonne National Lab (Co-PI), Nidhi Rastogi (Co-PI), 01/22-12/23.
- **RIT Grant Writerś Boot Camp Award– $5,000**, "Extracting threat intelligence signals from the Dark Web", Nidhi Rastogi (PI), 07/22-06/23.
- **RIT Testbed Initiative to Increase Research Competitiveness– $25,000**, "Data Generation for autonomous vehicle security", Nidhi Rastogi (PI), 07/22-06/23.
- **Toyota Infotech– $70,000**, "Unstable Explanations: A Challenge for Model Interpretation", Nidhi Rastogi (PI), 01/23-12/23.
- **INSuRE+C (Information Security Research and Education - Collaborative with NSA, Emergent (In)Security of Multi-Cloud Environments.) $65,000 (No F&A)**, NSA TD: Josiah Dykstra & Andy Sampson", Nidhi Rastogi (PI), Sudip Mittal (Co-PI), Summer 2023 funding to support 3 Students and Faculty.
- **IBM AI Research Collaboration– $200,000**, "Trust using Deep Learning in Cybersecurity", Nidhi Rastogi (PI), Mohammad Zaki & Alex Gittens (Senior Collaborator) 01/21-12/21.
- **IBM AI Research Collaboration– $150,000**, "Gathering Threat Intelligence for Trust in Cybersecurity", Nidhi Rastogi (PI), Mohammad Zaki & Alex Gittens (Senior Collaborator) 01/20-12/20.
- **IBM-RPI AIHN– $20 Million**, "Health Empowerment by Analytics, Learning, and Semantics (HEALS)", Nidhi Rastogi (Senior Collaborator) 01/17-12/22. My share ($150,000).

Applied. Total Value as PI, Co-PI,or Collaborator: $3,789,037

SOME TITLES HIDDEN SINCE PROPOSALS UNDER REVIEW

- **DARPA CASTLE– $8,578,000**, Team-TA3 (PI), Nidhi Rastogi (Co-PI), 06/22-07/27. My Share $1,635,309
- **DARPA CASTLE– $6,529,000**, Team-TA1 (PI), Nidhi Rastogi (Co-PI), 06/22-07/27. My Share $1,295,864.
- **SaTC: CORE: Small– $600,000**, "Dynamic and Open Knowledge Networks for Malware Threat Intelligence", Nidhi Rastogi (PI), 07/23-06/26. My share: $365,000
- **CAREER– $492,864**, "Towards Scalable, Contextual, and Trustworthy Cyber Threat Intelligence", Nidhi Rastogi (PI), 07/23-06/26.

Relevant Industry Appointments

GE Global Research

Niskayuna, NY

CYBERSECURITY RESEARCHER

Apr. 2010 - Dec. 2013

- Developed method for risk measurement and cyber-attack impact on energy grid Intelligent Electronic Devices (IEDs). Incorporated industry standards in research – NERC CIP, and IEC by performing in-depth literature study.
- Led and Co-led 2 projects and mentored 3 PhD students.

Verizon Wireless

Basking Ridge, NJ

MEMBER OF TECHNICAL STAFF, DEVICE TECHNOLOGY

Jan. 2009 - Apr. 2010

- Managed over-the-air device management for all Verizon wireless devices on LTE, 3G network, created road map by partnering with product management, OEMs, technology vendors to ensure compliance of requirements in devices using Verizon network.
- Identified rogue behavior in CDMA network and devices, quantified behavior thresholds, analyzed existing process of addressing issues, established ownership of process & reported-out the findings with recommendations to address gaps.

Honors and Awards

- **2022** 5K scholarship, Faculty Success Program by National Center for Faculty Development and Diversity.
- **2020** International Women in Cybersecurity by the Cyber Risk Research Institute, USA.
- **2016** FADEx laureate (10/160 selected), 1st French-American Program on Cyber-Physical Systems.
- **2016** 3rd place (out of 25), Datathon at Institute for Data Exploration and Application, RPI.
- **2014** Microsoft awarded ACM's SRC Travel Award for Grace Hopper.
- **2014** Anita Borg Institute Scholarship for Grace Hopper.
- **1999** National Mathematics Olympiad Award, India

Invited Talks and Panels

- **2022** "Scientifically Approaching Threat Intelligence", at Mississippi State University, July'22
- **2022** "New York University, Center for Cyber Security - Diversity, Equity, and Inclusion Panel", June'22
- **2022** "Context-driven Security: The need for a critical shift in attack detection", USENIX Enigma'22, Santa Clara, CA
- **2021** "Connected and Autonomous Vehicles", at the Workshop on Cyber Experimentation and the Science of Security
- **2021** "AI-bias in personal healthcare devices", panel discussion at Aspen Institute, Virtual
- **2021** "AI in Cybersecurity", at the Aspen Cyber Summit, Virtual
- **2019** Large Scale Cyberattack detection and User data Privacy in chat apps, MNIT, Jaipur, India.
- **2019** Cyberattack detection and Privacy of user data in large networks, Oracle Labs, Boston, MA.
- **2014** Towards Securer Networked Systems, Raytheon BBN, Boston MA.

Service

- **Committee**– Search Committee Member for the GCI Fellow, RIT 2021-22
- **Advisor**– Competition Judge, Society for Canadian Women in Science & Technology (SCWiST) Science Symposium'21.
- **Co-Chair**– ACSAC DYNAMICS Workshop co-Chair, 2020-21, 2023
- **PC**– Euro S&P'22, AAAI'21 Workshops, Reviewer for NSF'21, ACSAC DYNAMICS'19, ACSAC DYNAMICS'20, Knowledge Graph Conference - Personal Health Knowledge Graphs'20, many others
- **Reviewer**– Journal of Information Security and Applications (2020-), IEEE Transactions on Information Forensics and Security (2018-), AAAI Fall'20 AI for Social Good Symposium, Knowledge Graph Conference - Personal Health Knowledge Graphs'20, ACSAC DYNAMICS'19-'20, Book Chapter for "RDF and Knowledge Graph Provenance", Springer'20, IEEE Computer'18, ACM XRDS Articles'15-18, Student Program Committee at the 37th IEEE Symposium on S&P'16.
- **Advisor**– Adaptable Security Corp'19 (pro-bono), RIT Data Science Club (2022-), RIT WiCyS Chapter (2022-)
- **Board Member**– Lexington Education Foundation, MA 2019-21, N2Women'18-20. Society for Women Researchers in Communications & Networking (IEEE, ACM)

Teaching Experience

Rochester Institute of Technology (Fall'2021-Spring'23)

- Neural Networks, DSCI-640 *Spring'23*
- Foundations of Data Science, DSCI-633 *Fall'22*
- Applied Data Science, DSCI-601 *Fall'22*
- Foundations of Data Science, DSCI-633 *Fall'21*

Rensselaer Polytechnic Institute (Fall'13-Spring'18)

- Operating Systems and UNIX, CSCI 4210 Undergraduate & Graduate Level. *Fall'13*
- Operating Systems and UNIX, CSCI 4210 Undergraduate & Graduate Level. *Spring'14*
- Graph Theory and Analytics, CSCI 4260 Undergraduate & Graduate Level. *Fall'22*
- Operating Systems and UNIX, CSCI 4210 Undergraduate & Graduate Level. *Fall'17*

Advising

Rochester Institute of Technology (Fall'2021-Spring'23)

Committee Chair

- Md. Tanvirul Alam (Aug'21- Present), Ph.D. Graduate Researcher
- Dipkamal Bhusal (Aug'21- Present), Ph.D. Graduate Researcher
- Le Nguyen (Aug'21- Present), M.S. Data Science Researcher

Research Advisor

- Ajay Ashok Shewale (08/22- Present), M.S. Graduate Researcher on Explainable Security.
- Megha Gupta (01/22- 08/22), M.S. Graduate Researcher on Cyberthreat Intelligence.
- Praveen Chandrashekaran (08/22- Present), M.S. Graduate Researcher on Explainable Security.
- Rigved Rakshit (01/22- 08/22), M.S. Graduate Researcher on Explainable Security
- Omkar Chavan (12/22- Present), M.S. Graduate Researcher on Cyberthreat Intelligence.

Committe Member

- Morgan Reece (MSSTATE CSE, 2022 - Present), Ph.D. Graduate Researcher on Multi-Cloud Security
- Hrushikesh Mukherjee (University of Florida 08/22- Present), Ph.D. Graduate Researcher on Explainable Security.

Rensselaer Polytechnic Institute (Fall'2019-Present)

Committee Member

- Sharmishtha Dutta (01/20- Present), Ph.D. Graduate Researcher

Research Mentor for Undergraduates

- Ruisi Jian, Megan Goulet, Chuqiao Gu, Qicheng Ma, Destin Yee, Sean Hale, Jared Gridley, Aaron Hill, Lydia Zhou, Ryan Christian, Thomas Hopkins

Active Memberships

- Institute of Electrical and Electronics Engineers (IEEE)
- Association for Computing Machinery (ACM)
- IEEE Computer Society Technical Committee on Security and Privacy
- IEEE Blockchain

Press

- **India Proposes Chinese-Style Internet Censorship**, (02/19). Publisher: New York Times, India. Link: https://www.nytimes.com/2019/02/14/technology/india-internet-censorship.html
- **Is WhatsApp Really Unsafe And Is Signal Better Than WhatsApp?**, (01/20). Publisher: Huffpost. Link: https://www.piyasree-dasgupta.com/whatsapp-signal/4w74ukenvlo3e4tc2c1we4ppd34xh8
- **Contextual Security Should Supplement Machine Learning for Malware Detection**, (02/22). Publisher: Information Security Magazine. Link: https://www.infosecurity-magazine.com/news/contextual-security-machine/

Journal Publications, Conference Papers, and Book Chapters

1. Alam, M. T., Park, Y., & **Rastogi, N.**(2023). SoK: Towards Actionable Open Cyber Threat Intelligence. Under Review, ACM AsiaCCS'23.
2. Alam, M. T., Bhusal, D., Park, Y., & **Rastogi, N.** (2023). Looking Beyond IoCs: Automatically Extracting Attack Patterns from External CTI. Under Review, IEEE Euro S&P'23.
3. Nguyen, L, & **Rastogi, N.** (2023). Graph-based Approach for Studying Spread of Radical Online Sentiment. Under Review, The WebConf'23.
4. Bhusal, D., & **Rastogi, N.** (2023). SoK: Modeling Explainability in Security Monitoring for Trust, Privacy, and Interpretability. Under Review, IEEE Euro S&P'23.
5. Alam, M. T., Bhusal, D., & **Rastogi, N.** (2023). CyNER: A python library for cybersecurity named entity. Under Review, EMNLP'23. recognition. arXiv preprint arXiv:2204.05754.
6. Bhusal, D., & **Rastogi, N.** (2023). Building robust and resilient android malware classifiers: A survey on adversarial attacks and defenses. Under Review, Pattern Recognition.

7. Gloria, K., **Rastogi, N.**, & DeGroff, S. (2023). Bias impact analysis of ai in consumer mobile health technologies: Legal, technical, and policy. Under review, http://arxiv.org/abs/2209.05440.
8. **Rastogi, N.**, Dutta, S., Zaki, M., Gittens, A., & Aggarwal, C. (2022). TINKER: A framework for Open source Cyberthreat Intelligence. TrustCom'22.
9. **Rastogi, N.**, Rampazzi, S., Clifford, M., Heller, M., Bishop, M., & Levitt, K. (2022). Explaining RADAR features for detecting spoofing attacks in Connected Autonomous Vehicles. AAAI'22 Explainable Agency in Artificial Intelligence.
10. Chen, C.-H., Gruen, D., Harris, J., Hendler, J., McGuinness, D. L., Monti, M., **Rastogi, N.**, Seneviratne, O., & Zaki, M. J. (2022). Semantic technologies for clinically relevant personal health applications.
11. **Rastogi, N.** (2022). Contextual security: The need for a new paradigm in threat assessment. USENIX ENIGMA'22.
12. **Rastogi, N.**, & Hendler, J. A. (2022). Detecting systemic cyberattacks using Information Centrality in smart grid network. Under Review TIFS'22.
13. **Rastogi, N.**, Rampazzi, S., Clifford, M., Heller, M., Bishop, M., & Levitt, K. (2022). Explaining radar features for detecting spoofing attacks in autonomous vehicles. Under Review, AAAI'22 Workshop on Explainable Agency in Artificial Intelligence (EAAI'22).
14. Christian, R., Dutta, S., Park, Y., & **Rastogi, N.** (2021). Ontology-driven knowledge graph for Android malware detection. ACM CCS'21 Conference.
15. Yee, D., Dutta, S., **Rastogi, N.**, Gu, C., & Ma, Q. (2021). TINKER: Knowledge graph for threat intelligence. ACL-IJCLNP'21 Accepted.
16. **Rastogi, N.**, Dutta, S., Zaki, M. J., Gittens, A., & Aggarwal, C. (2020). MALOnt: An ontology for malware threat intelligence. SIGKDD'20 Workshop - International Workshop on Deployable Machine Learning for Security Defense, 28–44.
17. **Rastogi, N.**, & Ma, Q. (2020). DANTE: Predicting insider threat using lstm on system logs. The 19th IEEE International Conference on Trust, Security, and Privacy in Computing and Communications (IEEE TrustCom 2020).
18. **Rastogi, N.**, Seneviratne, O., Chen, Y. et al. (2020). Applying learning and semantics for personalized food recommendations. The 19th International Semantic Web Conference (ISWC 2020).
19. **Rastogi, N.**, & Zaki, M. J. (2020). Personal health knowledge graphs for patients. Workshop–Personal Health Knowledge Graphs (PHKG2020).
20. Haussmann, S., Chen, Y., Seneviratne, O., **Rastogi, N.**, Codella, J., Chen, C.-H., McGuinness, D. L., & Zaki, M. J. (2019). Foodkg enabled q&a application. ISWC Satellites, 273–276.
21. **Rastogi, N.** (2018a). Exploring information centrality for intrusion detection in large networks. 19th Annual Security Conference - Cybersecurity Workforce Development Challenges.
22. **Rastogi, N.** (2018b). A network intrusion detection system (NIDS) based on information centrality to identify systemic cyber attacks in large systems (Doctoral dissertation). Rensselaer Polytechnic Institute.
23. DiFranzo, D., Gloria, M. J. K., & **Rastogi, N.** (2017). Filter bubbles and fake news.
24. Divekar, R. R., & **Rastogi, N.** (2017a). Managing crises, one text at a time.
25. Divekar, R. R., & **Rastogi, N.** (2017b). Tech for crises.
26. **Rastogi, N.** (2017). Online censorship, cyberattacks, and access to information.
27. **Rastogi, N.**, & Divekar, R. R. (2017). Serving people in crisis to make the world a better place.
28. **Rastogi, N.**, & Hendler, J. (2017). WhatsApp security and role of metadata in preserving privacy. 12th International Conference on Cyber Warfare and Security, 6817, 269–275.

29. **Rastogi, N.**, & Hendler, J. (2016). Graph analytics for anomaly detection in homogeneous wireless networks-a simulation approach. arXiv preprint arXiv:1701.06823.

30. **Rastogi, N.**, & Scoică, A. (2016). The art and design of autonomous machines.

31. **Rastogi, N.**, Gloria, M. J. K., & Hendler, J. (2015). Security and privacy of performing data analytics in the cloud: A three-way handshake of technology, policy, and management. Journal of Information Policy, 5, 129–154.

32. **Rastogi, N.**, Zeng, Q.-A., & Li, X. (2011). Secure scheme during vertical handoff in integrated heterogeneous wireless systems. 2011 Wireless Telecommunications Symposium (WTS), 1–5.