

Nidhi Rastogi, Ph.D.

✉ iamnidhirastogi@gmail.com

🌐 nidhirastogi.github.io

📞 (781)-430-8685

Career Goals

Advancing Research and technology solutions leveraging Cybersecurity and Data Privacy, Knowledge Graphs, Artificial Intelligence, Machine Learning, Threat Modeling, Wireless Networks, Graph Analytics into solutions that influence Cybersecurity, Healthcare, and Autonomous Vehicle industries.

Enhancing Quality Learning for both in-person and remote education.

Education

- | | |
|-----------|---|
| 2013–2018 | Ph.D., Computer Science, Rensselaer Polytechnic Institute
Thesis Title: A Network Intrusion Detection System (NIDS) Based on Information Centrality to Identify Systemic Cyber Attacks in Large Systems
Supervisor: Dr. James A. Hendler |
| 2006–2008 | M.S., Computer Science, University of Cincinnati
Thesis Title: A Novel Security Scheme during Vertical Handoff in Integrated Heterogeneous Wireless Networks
Supervisor: Dr. Qing-An Zeng |
| 1999–2003 | Bachelor of Information Technology, University of Delhi |

Academic Appointments

- | | |
|-----------|--|
| 2019– | Research Scientist, IDEA, RPI |
| 2018–2019 | Post Doc, IDEA, RPI |
| 2018–2018 | Udacity - Online Course Instructor for MOOC, <i>Introduction to Cloud Security</i> .
Developed content, project instructions, created rubrics for assessing student work. Created and delivered video recorded content. |
| 2014–2018 | Research Assistant, Computer Science, RPI |
| 2016–2016 | Cybersecurity Researcher, GE Global Research, NY
Implemented Trusted Platform Module (TPM) in Linux to create a “Chain-of-Trust” for remotely located GE devices. |
| 2015–2015 | Graduate Researcher, IBM Research, Zurich
Experimented on IBM LAN using “centrality” approach to reduce overall analysis. |
| 2014–2014 | Intern, Raytheon BBN, Cambridge, MA
Fast Prototyping of threat model by creating ontologies for attacks in a tactical network. |
| 2013–2014 | Teaching Assistant, Computer Science, RPI
Operating Systems (3 sem), Graph Theory (1 sem) |

Funding

2021–2021	IBM AI Research Collaboration PI : Trust using Deep Learning in Cybersecurity, \$200,000
2021–2021	Silicon Valley Community Foundation (Cisco Research) co-PI : Generating Safe-Guards for AI Decision Making in Healthcare, \$100,000
2019–2020	IBM AI Research Collaboration PI : Gathering Threat Intelligence for Trust in Cybersecurity, \$150,000

Industry Appointments

2010–2012	Researcher - GE Global Research & GE Power, NY Designed a novel method of security 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.
2009–2010	Member of Technical Staff, Verizon, NJ Managed over-the-air device management for all Verizon wireless devices, created roadmap 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.

Awards and Honors

2020	International Women in Cybersecurity by the Cyber Risk Research Institute, USA
2016	FADEX laureate (10 out of 160 selected), 1st French-American Program on Cyber-Physical Systems
2016	3rd place (out of 25) at the 2016 Datathon, at Institute for Data Exploration and Application, Rensselaer
2015	IBM Summer Global Research Program, IBM Zurich
2014	Microsoft awarded ACM's SRC Travel Award for Grace Hopper
2014	Anita Borg Institute Scholarship for Grace Hopper

Supervision

Graduate	Sharmishtha Dutta (Ph.D.), Daniel Stevens (M.S.)
Undergrads	Ruisi Jian, Megan Goulet, Chuqiao Gu, Qicheng Ma, Destin Yee, Sean Hale, Jared Gridley, Aaron Hill, Lydia Zhou

Research Publications

Conference Proceedings

- 1 **Rastogi, N., & Hendler, J. A.** (2021). Detecting systemic cyberattacks using Information Centrality in large IP networks, In *Accepted - the 10th ACM Conference on Data and Application Security and Privacy (CODASPY'21)*.
- 2 Yee, D., Dutta, S., **Rastogi, N.**, Gu, C., & Ma, Q. (2021). Tinker: Knowledge graph for threat intelligence, In *Naacl'21 under review*.

- 3 **Rastogi, N.**, Dutta, S., Zaki, M. J., Gittens, A., & Aggarwal, C. (2020). MALOnt: An ontology for malware threat intelligence, In *International workshop on deployable machine learning for security defense*. Springer, Cham.
- 4 **Rastogi, N.**, & Ma, Q. (2020). Dante: Predicting insider threat using lstm on system logs, In *Accepted - the 19th IEEE International conference on trust, security and privacy in computing and communications (IEEE Trustcom 2020)*.
- 5 **Rastogi, N.**, & Zaki, M. J. (2020). Personal health knowledge graphs for patients, In *Workshop-personal health knowledge graphs (phkg2020)*.
- 6 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., In *Iswc satellites*.
- 7 **Rastogi, N.** (2018a). Exploring information centrality for intrusion detection in large networks, In *19th annual security conference - cybersecurity workforce development challenges*.
- 8 **Rastogi, N.**, & Hendler, J. (2017). Whatsapp security and role of metadata in preserving privacy, In *12th international conference on cyber warfare and security*.
- 9 **Rastogi, N.**, & Hendler, J. (2016). Graph analytics for anomaly detection in homogeneous wireless networks-a simulation approach.
- 10 **Rastogi, N.**, Zeng, Q.-A., & Li, X. (2011). Secure scheme during vertical handoff in integrated heterogeneous wireless systems, In *2011 wireless telecommunications symposium (wts)*. IEEE.

Journal Articles

- 1 **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.

Books and Chapters

- 1 McGuinness, D., **Rastogi, N.**, Seneviratne, O., Zaki, M., Harris, J., Gruen, D., & Chen, C.-H. (2021). Semantic technologies for enabling clinically relevant personal health applications, In *Reimagining personal health informatics for precision medicine and healthcare*. Springer.

Articles

- 1 DiFranzo, D., Gloria, M. J. K., & **Rastogi, N.** (2017). *Filter bubbles and fake news*.
- 2 Divekar, R. R., & **Rastogi, N.** (2017a). *Managing crises, one text at a time*. ACM New York, NY, USA.
- 3 Divekar, R. R., & **Rastogi, N.** (2017b). *Tech for crises*. ACM New York, NY, USA.
- 4 **Rastogi, N.** (2017). *Online censorship, cyberattacks, and access to information*. ACM New York, NY, USA.
- 5 **Rastogi, N.**, & Divekar, R. R. (2017). *Serving people in crisis to make the world a better place*. ACM New York, NY, USA.
- 6 **Rastogi, N.**, & Scoică, A. (2016). *The art and design of autonomous machines*. ACM.

Invited Talks

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

Co-Chair	ACSAC DYNAMICS Workshop co-Chair, 2020
Feature Editor	ACM XRDS (2016-2018)
PC	ACSAC DYNAMICS'19 ACSAC DYNAMICS'20 Knowledge Graph Conference - Personal Health Knowledge Graphs'20
Reviewer	IEEE Transactions on Information Forensics and Security (2018-Present) AAAI Fall'20 AI for Social Good Symposium Review Reminder Knowledge Graph Conference - Personal Health Knowledge Graphs'20 ACSAC DYNAMICS'20 ACSAC DYNAMICS'19 Book Chapter for "RDF and Knowledge Graph Provenance", Springer'20 IEEE Computer'18 ACM XRDS Articles'15-18 Student Program Committee at the 37 IEEE Symposium on S&P'16
Advisor	Adaptable Security Corp'19 (pro-bono)
Board Member	Lexington Education Foundation '19-Present, MA N2Women'18-20. Society for Researchers in Communications & Networking (IEEE, ACM)

References

Dr. James Hendler	Ph.D. Advisor. Professor, Rensselaer Polytechnic Institute, Troy, NY
Dr. Mohammad Zaki	Professor, Rensselaer Polytechnic Institute, Troy, NY
Dr. Michael Clifford	Principal Scientist, Toyota InfoTech Labs, Mountain View, CA
Dr. Charu Aggarwal	Distinguished Research Staff Member, IBM, NY