Nidhi Rastogi

Assistant Professor, Department of Software Engineering, Rochester Institute of Technology

nxrvse@rit.edu @nidhirastogi nidhirastogi.github.io nidhirastogi

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

2021–	Assistant Professor, Rochester Institute of Technology, NY
2019–2021	Research Scientist, IDEA, RPI
2018–2019	Post Doc, IDEA, RPI
2018–2018	Udacity - Online Course Instructor for MOOC, *Introduction to Cloud Security*.
	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

2022–	Toyota InfoTech Labs Research Collaboration, **$70,000**
	PI : Explainable Security in Autonomous Vehicles
2021–2021	IBM AI Research Collaboration, **$200,000**
	PI : Trust using Deep Learning in Cybersecurity
2021–2021	Silicon Valley Community Foundation (Cisco Research), **$100,000**
	co-PI : Generating Safe-Guards for AI Decision Making in Healthcare
2019–2020	IBM AI Research Collaboration, **$150,000**
	PI : Gathering Threat Intelligence for Trust in Cybersecurity
2017–2022	IBM-RPI AIHN, **$20 million**
	Collaborator : Health Empowerment by Analytics, Learning, and Semantics (HEALS)

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 on LTE, 3G network, 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

2022	5K scholarship to attend the Faculty Success Program run by the National Center for Faculty Development and Diversity
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
1999	National Mathematics Olympiad Award, India

Supervision

Ph.D.	Md. Tanvirul Alam, Dipkamal Bhusal
M.S.	Praveen Chandrasekaran, Megha Gupta, Le Nguyen, Rigved Rakshit
Alumni	Sharmishtha Dutta (Ph.D. at RPI), Undergraduates - Ruisi Jian, Megan Goulet, Chuqiao Gu, Qicheng Ma, Destin Yee, Sean Hale, Jared Gridley, Aaron Hill, Lydia Zhou, Ryan Christian, Thomas Hopkins

Publications

1. **Rastogi**, **N.** Contextual security: A critical shift in performing threat intelligence. In: Santa Clara, CA: USENIX Association, 2022, February.
2. Alam, M. T., Bhusal, D., & **Rastogi**, **N.** (2022). CyNER: A python library for cybersecurity named entity recognition. *Under Review NAACL-Demo'22*.
3. Bhusal, D., & **Rastogi**, **N.** (2022). Building robust and resilient android malware classifiers: A survey on adversarial attacks and defenses. *Under Review, IEEE Transactions on Dependable and Secure Computing- Special Issue on Reliability and Robustness in AI-Based Cybersecurity Solutions*.
4. **Rastogi**, **N.** (2022b). Contextual security: The need for a new paradigm in threat assessment. *USENIX ENIGMA'22*.
5. **Rastogi**, **N.**, Alam, M. T., Dutta, S., Bhusal, D., Gittens, A., Zaki, M. J., & Aggarwal, C. (2022). Triaging android malware threats using knowledge graphs. *Under Review, IEEE TIFS'22*.
6. **Rastogi**, **N.**, & Hendler, J. A. (2022). Detecting systemic cyberattacks using Information Centrality in smart grid network. *Under Review TIFS'22*.
7. **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)*.
8. Christian, R., Dutta, S., Park, Y., & **Rastogi**, **N.** (2021). Poster: Ontology-driven knowledge graph for android malware detection. *ACM CCS'21 Conference*.
9. McGuiness, D., **Rastogi**, **N.**, Seneviratne, O., Zaki, M., Harris, J., Gruen, D., & Chen, C.-H. (2021). Semantic technologies for enabling clinically relevant personal health applications. *Reimagining personal health informatics for precision medicine and healthcare*. Springer.
10. **Rastogi**, **N.** (2021). *Semantic technologies for enabling clinically relevant personal health applications*.
11. Yee, D., Dutta, S., **Rastogi**, **N.**, Gu, C., & Ma, Q. (2021). TINKER: Knowledge graph for threat intelligence. *ACL-IJCLNP'21 Accepted*.
12. **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.
13. **Rastogi**, **N.**, & Ma, Q. (2020). DANTE: Predicting insider threat using lstm on system logs. *Accepted - The 19th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (IEEE TrustCom 2020)*.
14. **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)*.
15. **Rastogi**, **N.**, & Zaki, M. J. (2020). Personal health knowledge graphs for patients. *Workshop–Personal Health Knowledge Graphs (PHKG2020)*.

16 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*.

17 **Rastogi**, **N.** (2018a). Exploring information centrality for intrusion detection in large networks. *19th Annual Security Conference - Cybersecurity Workforce Development Challenges*, http–029e2c6.

18 **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.

19 DiFranzo, D., Gloria, M. J. K., & **Rastogi**, **N.** (2017). *Filter bubbles and fake news.*

20 Divekar, R. R., & **Rastogi**, **N.** (2017a). *Managing crises, one text at a time*.

21 Divekar, R. R., & **Rastogi**, **N.** (2017b). *Tech for crises*.

22 **Rastogi**, **N.** (2017). *Online censorship, cyberattacks, and access to information*.

23 **Rastogi**, **N.**, & Divekar, R. R. (2017). *Serving people in crisis to make the world a better place*.

24 **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.

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

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

27 **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.

28 **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.

Invited Talks and Panels

2022	"Context driven Security: The need for a critical shift in attack detection", at the USENIX Enigma'22, Santa Clara, CA
2021	"Connected and Autonomous Vehicles", at the Workshop on Cyber Experimentation and the Science of Security (CESoS), Virtual
2021	"AI-bias in personal healthcare devices", panel discussion at Aspen Inctitute, 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.

Posters and Presentations

2021	"Knowledge Graphs for Cyber threat Intelligence", at the Great Lakes Security Day, virtual
2021	ACM CCS - Ontology-driven Knowledge Graph for Android Malware,
2021	ASPEN Cyber Summit, "Machines within Machines: Artificial Intelligence in Cyberspace"
2020	SANS Security - Automated Detection of Software Vulnerabilities Using Deep-Learning,
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 Committe Member for the GCI Fellow, RIT
Adviser	Competition Judge for the Society for Canadian Women in Science & Technology (SCWiST) Science Symposium
Co-Chair	ACSAC DYNAMICS Workshop co-Chair, 2020-22
Feature Editor	ACM XRDS (2016-2018)
PC	ACSAC'22, 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'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 2019-21, MA
	N2Women'18-20. Society for Researchers in Communications & Networking (IEEE, ACM)