Nidhi Rastogi, Ph.D.

Boston, MA | 513.417.7449| iamnidhirastogi@gmail.com | linkedin.com/in/rastoginidhi| GitHub: nidhirastogi

RESEARCHER

Over 8 years of progressive experience in creating research solutions leveraging Cyber Security, Artificial Intelligence, Machine Learning, Threat modeling, Networks, Graph Theory into solutions that influence Healthcare, Cybersecurity, and Network industries. Experienced in building projects from concept to prototype, establishing requirements for large scale technology deployment; Leading teams, and advising post-docs, PhDs.

EDUCATION

Ph.D., Computer Science, *Rensselaer Polytechnic Institute,* NY, USA   2018

Thesis Advisor: Dr. James Hendler, GPA: 3.9/4.0

M.S. in Computer Science, *University of Cincinnati,* OH, USA   2009

Bachelor of Information Technology, *University of Delhi,* Delhi, India   2003

TEACHING EXPERIENCE

Cybersecurity Online Instructor | UDACITY   2018

Teaching Assistant - CSCI 4210, 6210, Operating Systems at RPI   2013-15

PROFESSIONAL EXPERIENCE

RESEARCH SCIENTIST | RENSSELAER POLYTECHNIC INSTITUTE   Troy, NY   09/19-Present

Leading or Co-leading research projects (1m – 150k grant) in different capacities. Demo lead for HEALS (Health Empowerment by Analytics, Learning, and Semantics) that applies advanced cognitive computing capabilities to monitor patients ensuring personalized solutions. PI for Deep Threat Intelligence.

Key Accomplishments:

- Leading demonstration of Phase II: HEALS for patient facing mobile app to senior executives at IBM and PIs at RPI with next-gen AI technology encompassing Personalization, Explainability, and Conversation technologies.
- PI for "AI Models for Curation of Threat Intelligence" as the Security Analytics SME, creating roadmap for identifying and managing existing gaps in IBM SIEM platform. Using Machine Learning, Ontologies, Knowledge Graphs, NLP.
- Advising PhDs, recruiting undergraduates and advising on research and engineering aspects per project's short term requirements.

Postdoctoral Research Associate | RENSSELAER POLYTECHNIC INSTITUTE   Troy, NY   12/18-08/19

Demo lead for HEALS (Health Empowerment by Analytics, Learning, and Semantics) that applies advanced cognitive computing capabilities to monitor patients ensuring personalized solutions.

Key Accomplishments:

- Led successful demonstration of Phase I: HEALS for patient facing mobile app to senior executives at IBM and PIs at RPI. Renewed sponsors' faith in research and 1m funding for next fiscal year.
- Advising PhDs working on Knowledge Base Question Answering, building personalized health solutions for patients – both in food choices and physical activity recommendations.
- Collaborating with a large, geographically distributed team of senior researchers, software engineers, PhDs and postdocs to prioritize and deliver quarterly/annually defined goals.
- Present research updates, findings and project status to senior leaders at RPI, IBM.

CYBERSECURITY Instructor | UDACITY   Mountain View, CA   07/18-11/18

Created online courses for industry professionals, and students across the world to gain essential job ready skills.

Key Accomplishments:

- Led 5 content developers with non-security background into building online cloud security course.
  o Helped gain technical clarity in content required to build the course – All lessons and projects.

- o Drafted project instructions and created rubrics for assessing student work fairly and completely per Udacity defined rubrics; recommended several updates.
- o Created and delivered video recorded content including headshots and screencasts.
- Collaborated with SMEs from leading Tech companies (Facebook, Atlassian, VMWare), identified skills for SDEs and mapped them to curriculum.

GRADUATE RESEARCHER | RENSSELAER POLYTECHNIC INSTITUTE   Troy, NY   01/13-07/18

- Researched attack scenarios – Insider Threat, Anomaly Detection, DDoS detection using multiple datasets sourced from "*Impact Cyber Trust*" data repository.
- Collaborated w/ Industry partners on various projects – ML classification, prediction models using JSON datasets (10GB-.5TB) with RESTful APIs. Explored deep-learning algorithms. Scaled up deployment using Docker containers, and nginx load balancers, ELB in AWS EC2. *Tools – Jupyter notebook, python2.7, scikit-learn, Postman, curl, Docker, TensorFlow.*
- Participated in several CTFs as part of the RPISEC team - resident computer security club at RPI.
- **Thesis**- Threat and attack detection in large networks by identifying systemic anomalous behavior. Identified anomalous data from a set of "important" nodes (instead of an entire system) leveraging Graph Analytics and Machine Learning tools. Used simulated (NS2) and real attack dataset. Quantified impact of proposed model & compared with PCA-based anomaly detection.
- 3rd place (25 teams), Machine Learning Datathon using World Bank dataset, IDEA Labs@ RPI, Troy, May'16.
- Evaluated 3 approaches in cybersecurity realm and their applications through diverse summer projects:
  - o *GE Global Research Intern, NY* - Implemented Trusted Platform Module (TPM) in Linux to create a "Chain-of-Trust" for remotely located GE devices.
  - o *IBM Research, Intern, Zurich* - Experimented on IBM LAN using "centrality" approach to reduce overall analysis. #endpoints – 3500, Links >10K. *Tools – Jupyter notebook, NetworkX, NetFlow v9.*
  - o *Raytheon BBN Technologies* - Fast Prototyping of threat model by creating ontologies for attacks in a tactical network. Client – Air Force research lab. *Tools – STRIDE, Attack Graphs, Java, Sparql.*
- **Publications** – 5 (+1 accepted) peer-reviewed publications and 8 articles.

SENIOR SOFTWARE ENGINEER | LOGIC TECHNOLOGIES Inc.   Schenectady, NY   04/10-12/12

As contracted researcher and engineer at GE Global Research and GE Power, worked on diverse engineering and research projects spanning networking, security and software technologies.

Key Accomplishments

- Designed a novel method of security measurement and cyber-attack impact on energy grid assets. Evolved it to extend across other Intelligent Electronic Devices (IEDs) in the grid. Incorporated industry standards in research - NERC CIP, and IEC by performing in-depth literature study
- Modeled and simulated prototype design using Java (for GUI) and GE internal language (used to build semantic models and authoring rules.)
- Led software development for financial analytics tool, and transitioned databases. Tools: MySQL, SQL.

Member of Technical Staff - Network & Technology | VERIZON   Basking Ridge, NJ   01/09-04/10

Led LTE/4G and CDMA technology development - Over-the-Air (OTA) device updates

Key Accomplishments

- Created design requirements (12) and test plans (6) for mobile device development & qualification. Performed device testing to ensure functionality over network.
- SME for OTADM, created roadmap by partnering with product management, OEMs, technology vendors to ensure compliance of requirements in devices using Verizon network.

- Rogue Device Management - 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.
- Led project communication of team on status, validation & business impact to leadership team.

PUBLICATIONS

- **Presentations & Publications**
  - o "MALOnt: An Ontology for Malware Threat Intelligence", MLHat Workshop at SIGKDD'20, Virtual
  - o "Personal Health Knowledge Graphs for Patients", 1st Personal Knowledge Workshop, Knowledge Graph Conference, New York, 2020.
  - o "FoodKG Enabled Q&A Application", The 18th International Semantic Web Conference, 2019.
  - o "A Network Intrusion Detection System (NIDS) Based on Information Centrality to Identify Systemic Cyber Attacks in Large Systems." PhD diss., Rensselaer Polytechnic Institute, 2018.
  - o "Exploring Information Centrality for Intrusion Detection in Large Networks", 17th Annual Security Conference, March 23-25 2018, Las Vegas, NV.
  - o "WhatsApp Security and role of metadata in preserving Privacy," 12th International Conference on Cyber Warfare and Security 2017 Proceedings (Link).
  - o "Security and Privacy of Performing Data Analytics in the Cloud: A Three-way Handshake of Technology, Policy, and Management" Journal of Information Policy, 2015 (Link).
  - o "Secure scheme during vertical handoff in integrated heterogeneous wireless systems." IEEE Wireless Telecommunications Symposium (WTS) 2011 (Link).
  - o GHC Security Track, 2014 – "Approaches to Malware detection and Analysis".
- **Posters**
  - o "Exploring Graph Centralities for Detecting Anomalous Behavior in Large Networks", Trust and Trustworthy Computing: 8th International Conference, TRUST 2015, Greece (Link).
  - o ACM GHC Student Research Competition, 2014 (*Quarter Finalist*) – "Malware Analysis with Architectural Approach"
- **Research Articles**
  6 articles for XRDS: Crossroads, ACM. Interviewed technology luminaries in Security, Robotics, Privacy. 2016-17.
  - o Online censorship, cyberattacks, and access to information, 2017
  - o Managing crises, one text at a time, 2017
  - o Filter bubbles and fake news, 2017
  - o Tech for crises, 2017
  - o Serving people in crisis to make the world a better place, 2017
  - o The art and design of autonomous machines, 2016

INVITED TALKS & PRESENTATIONS

- "Deep Learning for detecting software vulnerabilities", SANS Security, June 2020.
- "Towards Securer Networked Systems," May 2014, Raytheon BBN, Boston MA.
- "Cyberattack detection and Privacy of user data in large networks," June 2019, Oracle Labs, Boston, MA.
- "Large Scale Cyberattack detection and User data Privacy in chat apps," July 2019, MNIT, Jaipur, India.

RESEARCH & LEADERSHIP ACTIVITIES

Reviewer

- IEEE Transactions on Information Forensics and Security, Invited Reviewer, 2019 -20 (Impact factor – 6.211)
- Student Program Committee at the 37th IEEE Symposium on Security & Privacy, 2015-16(*Impact Factor 1.596*).
- DYNAMICS Workshop Committee Member, ACSAC Conference, 2019 (Top 5 Security Conference)
- DYNAMICS Program and Review Committee Member, ACSAC Conference, 2019 (Top 5 Security Conference)
- IEEE Computer 2018, Reviewer. (Impact factor – 0.98)

Leadership/Volunteer Activities

- Security Advisor, pro-bono, Adaptable Security Corp, 2019
- Board Member (Advisor for Technology and Strategy) (2019-Present)– Lexington Education Foundation, MA.
- Board Member (N2Women 2018-20): Society for Researchers - Communications & Networking (IEEE, ACM).
- Feature Editor, ACM XRDS Magazine http://xrds.acm.org/, September'15 – December'17.
- Teaching Assistant – Operating Systems & Programming (Spring'13,'14, Fall'14), Graph Theory (Fall'14)

AWARDS

- International Woman in Cybersecurity, Cyber Institute, April 2020.
- 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, RPI, Troy, 2016.
- Selected for IBM Summer Global Research Program, IBM Zurich, 2015.
- Microsoft awarded ACM's SRC Travel Award for Grace Hopper, 2014.
- Anita Borg Institute Scholarship for Grace Hopper, 2014.
- National Mathematics Olympiad winner, India, 1996.