

# Arushi Arora

Github: <https://github.com/noodlehair-git>

Linkedin: <https://www.linkedin.com/in/arorarushi/>

arushi1250@gmail.com

+1 (765)-775-8140

---

*Experienced researcher in the field of cybersecurity, with expertise in privacy preserving systems, SBoMs, anonymous communication protocols, information & network security, and applied cryptography. 4+ years in academia, working on cutting-edge projects and publications with over 210 citations on [Google Scholar](#).*

## Academic Experience

**Ph.D., Computer Science** (GPA 4.0/4.0)

[Purdue University](#)

**Activities and societies:** Research Assistant

**May'24 (expected)**

West Lafayette, IN

**M.S., Computer Science** (GPA 3.96/4.0)

[Purdue University](#)

**Activities and societies:** Research Assistant, Teaching Assistant

**2021**

West Lafayette, IN

**B.Tech., Computer Science** (Gold Medalist) (Percentage: 90.26%)

[Indira Gandhi Delhi Technical University](#)

**Activities and societies:** Research Assistant

**2019**

New Delhi, India

## Professional Experience

**Graduate Cybersecurity Researcher**

[National Renewable Energy Laboratory](#)

*Introduced privacy-preserving properties to Distributed Energy Resources (DER) network and Cyber-Informed Engineering (CIE) principles for clean energy systems.*

- Developing a **privacy-preserving DER network** by incorporating anonymous credentials, ensuring enhanced privacy and confidentiality within the network.
- Designing and implementing a mechanism to enable DER components to prove their non-vulnerability through **set non-membership zero-knowledge proofs**, bolstering the security of the network.
- Introducing **CIE principles** to a clean energy system based on the DER lifecycle.
- Conducting comprehensive attack simulations to evaluate the impact of implementing CIE principles within a DER network, quantifying the reduction in the attack surface, and enhancing the network's overall security.

**05/2023 - Present**

Denver, CO

---

**Ph.D. Researcher, National & Homeland Security**

[Idaho National Laboratory](#)

*Conducted research on Software Bill of Materials (SBoM), with a focus on privacy-compliant and vulnerability disclosure practices.*

- Designed and implemented the first notion of **privacy preserving SBoM system**, detailing its security properties and components, presented a concrete implementation based on **Private Set Intersection (PSI)**.
- Demonstrated the practicality of the devised privacy preserving SBoM system with real-world integration, benchmarks, and deployment consideration with an in-depth information leakage (security) analysis.
- Investigated **state-of-the-art SBoM tools** by creating a framework for analysis, categorizing **83 open-source tools** based on chosen features and functionalities and providing a detailed analysis and recommendations for tool selection to promote understanding and adoption of SBoMs and pave a path for future work in the field.

**08/2021 – 05/2023**

Idaho Falls, ID

---

**Graduate Research Assistant**

[Purdue University](#)

Prof. [Christina Garman](#)

*Led the development of programmable anonymity networks, extensions of Tor that enable users to run code on Tor routers, to build more advanced and secure anonymous services. ([website](#)) ([github](#))*

- Designed and implemented a **CDN** for the Tor anonymity network, resulting in a **56.4%** reduction in onion service download times and conducted a comprehensive security analysis.
- Developed a framework for enhancing onion service performance through **multipath routing**, resulting in a significant decrease in client-side time-to-first byte.
- Devised, implemented, and evaluated the **first provable geographic avoidance** system for onion services, resulting in successful proof of avoidance in multiple regions.
- Developed, deployed and stress-tested a **load balancer** for the Tor anonymity network, which automatically scales onion service replicas to handle varying load, resulting in a notable improvement in client-side performance.

**01/2020 - Present**

West Lafayette, IN

---

## Visiting Researcher

[The University of Melbourne](#)

Created Atomic Cross-chain Exchange (ACE), a decentralized, blockchain-based mechanism for Inter-Blockchain Communication on the Ethereum network.

05/2018 - 08/2018

Melbourne, Australia

---

## Research Intern

[University of Technology Sydney](#)

Dr. [Nisha Saroha Malik](#)

Devised a framework for enhancing the security and robustness of mobile networks, specifically Vehicular Ad-hoc Networks, using Blockchain.

10/2017 - 04/2018

Sydney, Australia

---

## Publications ([Google Scholar](#))

- Arora, Arushi, Christina Garman, and Dave Levin. "Improving the Performance and Security of Tor's Onion Services." 2023. (*under review*)
  - Arora, Arushi, Raj Karra, Dave Levin, and Christina Garman. "Provably Avoiding Geographic Regions for Tor's Onion Services." The Financial Cryptography and Data Security 2023 (FC '23). 2023. ([link](#))
  - Arora, Arushi, Virginia Wright, and Christina Garman. "Privacy preserving Software Bill of Materials." 2023. (*under review*)
  - Arora, Arushi, Virginia Wright, and Christina Garman. "SoK: A Framework for and Analysis of Software Bill of Materials Tools." Cyber Security: A Peer-Reviewed Journal. 2023. (*accepted, in publication*)
  - Arora, Arushi, Virginia Wright, and Christina Garman. "Strengthening the Security of Operational Technology: Understanding Contemporary Bill of Materials." JCIP The Journal of Critical Infrastructure Policy 3.1 (2022): 111. ([link](#))
  - Reininger, Michael, Arushi Arora, Stephen Herwig, Nicholas Francino, Jayson Hurst, Christina Garman, and Dave Levin. "Bento: Safely bringing network function virtualization to Tor." In Proceedings of the 2021 ACM SIGCOMM 2021 Conference, pp. 821-835. 2021. ([link](#))
  - Malik, Nisha, Priyadarsi Nanda, Arushi Arora, Xiangjian He, and Deepak Puthal. "Blockchain based secured identity authentication and expeditious revocation framework for vehicular networks." In 2018 17th IEEE international conference on trust, security and privacy in computing and communications/12th IEEE international conference on big data science and engineering (TrustCom/BigDataSE), pp. 674-679. IEEE, 2018. ([link](#))
  - Arushi, Arora, and Yadav Sumit. "Blockchain Based Security Mechanism for Internet of Vehicles (IoV)." SSRN Electronic Journal (2018). ([link](#))
  - Arora, Arushi, Sumit Kumar Yadav, and Kavita Sharma. "Denial-of-service (dos) attack and botnet: Network analysis, research tactics, and mitigation." In Research Anthology on Combating Denial-of-Service Attacks, pp. 49-73. IGI Global, 2021. ([link](#))
  - Arora, Arushi, and Sumit Kr Yadav. "Batman: Blockchain-based aircraft transmission mobile ad hoc network." In Proceedings of 2nd International Conference on Communication, Computing and Networking, pp. 233-240. Springer, Singapore, 2019. ([link](#))
  - Yadav, Sumit Kumar, Kavita Sharma, and Arushi Arora. "Security integration in DDoS attack mitigation using access control lists." International Journal of Information System Modeling and Design (IJISMD) 9, no. 1 (2018): 56-76. ([link](#))
  - Yadav, Sumit Kumar, Kavita Sharma, Chanchal Kumar, and Arushi Arora. "Blockchain-based synergistic solution to current cybersecurity frameworks." Multimedia Tools and Applications (2021): 1-22. ([link](#))
- 

## Program Committees

- [Program Committee](#), ACM S3 2023 Workshop, at 29th Annual International Conference on Mobile Computing and Networking (MobiCom'23), Madrid, Spain.
  - [Artifact Evaluation Committee](#), The 29th ACM Symposium on Operating Systems Principles (SOSP'23), Koblenz, Germany.
  - [Artifact Evaluation Committee](#), 19th International Conference on emerging Networking Experiments and Technologies (CoNext'23), Paris, France.
  - Mentor at [Hackillinois'23](#), annual collegiate hackathon and technology conference that takes place at the University of Illinois at Urbana-Champaign.
- 

## Travel Grants

- [Financial Cryptography and Data Security 2023 \(FC'23\)](#), Bol, Brač, Croatia.
- [ACM Special Interest Group on Data Communication \(SIGCOMM'23\)](#), New York, US.
- [23rd Privacy Enhancing Technologies Symposium \(PETS'23\)](#), Lausanne, Switzerland.
- [20th USENIX Symposium on Networked Systems Design and Implementation, \(NSDI'23\)](#), Boston, MA, USA.

---

## Awards & Achievements

- **Best Poster Presentation NDSS (2022)** for Improving the Performance and Security of Tor's Onion Services.
- **SIGCOMM'23 N2Women Fellowship**.
- Over **200+** citations on Google Scholar for research publications in top-tier journals and conferences.
- **Chancellor's Gold Medal (2019)**, **Vice Chancellor's Gold Medal (2019)**, and **Exemplary Performance (2019)** awards for outstanding academic achievement in Computer Science (Bachelor of Technology).

---

## Skills, Tools, & Language

- Cybersecurity, Network & Information Security, Applied Cryptography, Networks & Communication, Anonymous Communication, Security & Privacy
- Tor, Snort, SGX, Stem for Tor, OpenSSL, John the Ripper, Hashcat, AWS, Graphene-SGX
- Python, Linux, SQL, Git, C, HTML
- **Relevant coursework:** Algorithms, Computer Networks, Information security, Cryptography, Programming Languages, Intrusion detection systems, Economic & legal aspects of security, Passwords & authentication, Analysis of SGX SDKs

---

## Side Projects

- **SGX-Tor:** Designed and implemented a secure and private version of Tor using Intel SGX for a trusted execution environment.
  - **Resource Footprint of the Snort IDS:** Conducted an in-depth analysis of Snort IDS performance, examining the impact of Snort rules on detecting malicious traffic and identifying key factors for optimization.
  - Closing the Gap- **Hybrid Password Cracking:** Developed and implemented a hybrid approach to close the gap between perfect knowledge and state-of-the-art password cracking attacks, resulting in a more efficient and effective method for cracking passwords.
  - Created a blockchain-based **global identity ledger** using the Ethereum framework, aimed at preventing women and child trafficking.
  - Modified **OpenSSL** codes and developed necessary wrapper functions to enable SGX-protected applications to utilize OpenSSL library securely.
  - Evaluated the performance of Redis and Memcached on **Graphene-SGX**, providing insights on the suitability of the in-memory data stores for SGX-protected environments.
  - Designed and developed network applications such as **VPN, Overlay Network and Audio Streaming** using C programming language.
-