

# Aqsa Kashaf

(412) 636-4572 | [akashaf@cmu.edu](mailto:akashaf@cmu.edu) | [webpage](#)

## EDUCATION

### Carnegie Mellon University

*PhD Student, Electrical And Computer Engineering Department (ECE)*

**Advisor:** [Vyas Sekar](#), [Yuvraj Agarwal](#)

**Relevant Courses:** Network Security (18-731), Introduction to Machine Learning (10-701), Programmable Networks (15-829), Secure Software Systems (18-732), Network Economics, Advanced Operating Systems (15-712), Sensing and IoT (17-881), Advanced Topics in Machine Learning and Game Theory (17-759)

### LUMS University

*BS in Computer Science*

Pittsburgh, PA

*Aug. 2016 - May 2023*

Lahore, Pakistan

*Aug. 2012 - May 2016*

## PROFESSIONAL EXPERIENCE

### Network Software Engineer, SDN team, ByteDance | 2023-

- Worked on building high availability TE controller for the china DCs
- Worked on implementing a soft-isolation service in ByteDance's global BBone network

## PROJECTS

### Building an Internet Observatory for Africa | *On-going*

- Building a control layer to orchestrate existing measurement tools and platforms for an Internet observatory

### Estimating the Resource Constraints of a DDoS Defence System | *Under-review*

- Remote Profiling of the processing capacity of Network Functions deployed in a DDoS Defence System
- Implemented a tool called NFTY to estimate the processing capacity of stateless network functions
- **Skills:** Machine learning, system engineering, network tomography, packet analysis, IDS (Snort, Suricata), Firewalls (Fortinet, Firehol), DDoS Mitigation functions, AWS (VPC, Subnets, topology), GCP, Linux networking stack, kernel performance optimizations, DPDK, threat modeling, docker, scapy, libpcap

### Analysing Third Party Service Dependencies | *Published*

- Analysed the prevalence of third-party DNS, CDN and CA dependencies in modern web services
- Studied centralization among service providers
- **Skills:** Internet measurements, DNS, CDN, and WebPKI Infrastructure, Web Dashboard, Web scraping, dependency analysis, graph analysis, temporal analysis, data analysis, data visualization, D3

### Formal Verification of Smart Home Applications | *Published*

- Designed and developed a formal verification tool for smart home applications to identify safety violations
- Modelled smart home applications using timed automata (TA) and built a parser to translate apps into TA.
- **Skills:** Code parser, system building, model checking, real-time modeling abstractions, safety properties specifications, test case formulation, unit testing, ground truth validation, modeling using automata, selenium, performance benchmarking, fuzzing

### Zeus: Performant DDoS Protection System using multiple dataplanes

- Worked on designing the control layer of Zeus which assigned incoming benign and attack traffic to the most cost-effective dataplane among programmable switches, virtual machines, GPUs, FPGAs
- Worked on the attack mitigation logic for different application layer and network layer attacks
- Worked on devising mitigation schemes in the control plane against a reconnaissance attack
- **Skills:** ILP, Optimization, DDoS mitigation functions, Gurobi

### Incantivizing Censorship Measurements with Circumvention | *Published*

- Designed and developed a platform to measure censorship in real-time and provide adaptive circumvention.
- **Skills:** Internet Measurements, user application, MongoDB, NodeJS, OSI layers, censorship techniques and circumvention, BGP routing, asynchronous programming

### Mitigating Incast Congestion using RTO Randomization | *Published*

- Studied the impact of MIN\_RTO randomization on incast congestion using NS2 simulations
- **Skills:** Datacenter networking, NS2

## TECHNICAL SKILLS

**Languages:** C, C++, Java, MATLAB, Python, Go, Lua, Node.js, Assembly Language, TCL, MySQL, JavaScript, Ruby, HTML, CSS, UNIX Shell scripts, Groovy, OCaml

**Frameworks:** Docker, Suricata, Snort, Click Router, DPDK, AWS, Linux networking stack, Gurobi, Mininet, OpenFlow, Scikit learn, numpy, scipy, matplotlib, Network Simulator (NS2)

**Knowledge:** Applied Cryptography, Static analysis techniques, runtime analysis techniques, differential privacy, machine learning, network attacks, application layer attacks, web security, Integer linear programming, TCP/IP, UDP, Routing protocols like BGP

## HONORS AND AWARDS

---

EECS Rising Star	2022
Internet Research Task Force (IRTF) Applied Networking Research Prize	2021
Grace Hopper Celebration (GHC) Scholar	2016
Carnegie Institute of Technology Dean's Fellow	2016

## PUBLICATIONS

---

- [1] **A First Look at Third-Party Service Dependencies of Web Services in Africa**  
Aqsa Kashaf, Jiachen Dou, Margarita Belova, Maria Apostolaki, Vyas Sekar, Yuvraj Agarwal  
In *Proceedings of the Passive and Active Measurement Conference (PAM)*, 2023
- [2] **Protecting Smart Homes from Unintended Application Actions**  
Aqsa Kashaf, Vyas Sekar, Yuvraj Agarwal  
In *Proceedings of the IEEE/ACM International Conference on Cyber-physical Systems (ICCPS)*, 2022
- [3] **Analyzing Third Party Service Dependencies in Modern Web Services: Have We Learned from the Mirai-Dyn Incident? [IETF/IRTF Applied Networking Research Prize winner](#)**  
Aqsa Kashaf, Vyas Sekar, Yuvraj Agarwal  
In *Proceedings of the ACM Internet Measurement Conference (IMC)*, 2020
- [4] **Incentivizing censorship measurements via circumvention.**  
Aqib Nisar, Aqsa Kashaf, Ihsan Ayyub Qazi, and Zartash Afzal Uzmi  
In *Proceedings of the 2018 Conference of the ACM Special Interest Group on Data Communication (SIGCOMM)*, 2018.
- [5] **Training on Foveated Images Improves Robustness to Adversarial Attacks**  
Muhammad Shah, [Aqsa Kashaf](#), and Bhiksha Raj.  
Advances in Neural Information Processing Systems (NeurIPs) 2024
- [6] **A case for marrying censorship measurements with circumvention.**  
Aqib Nisar, [Aqsa Kashaf](#), Zartash Afzal Uzmi, and Ihsan Ayyub Qazi.  
In *Proceedings of the 14th ACM Workshop on Hot Topics in Networks (HotNets)*, 2015.
- [7] **Mitigating datacenter incast congestion using rto randomization**  
Ubaid Ullah Hafeez, [Aqsa Kashaf](#), Aisha Mushtaq, Hassan Zaidi, Ihsan Ayyub Qazi, and Zartash Afzal Uzmi.  
In *Proceedings of IEEE Global Communications Conference (GLOBECOM)*, 2015.

## REVIEW EXPERIENCE

---

Program Committee of ACM IMC 2023  
Program Committee of SIGCOMM Poster Session 2023  
Program Committee of Passive and Active Measurement Conference 2024  
Program Committee of Passive and Active Measurement Conference 2022  
Shadow Program Committee of IEEE Security and Privacy 2021  
Artifact Evaluation of Operating Systems Design and Implementation 2021

## TEACHING ASSISTANTSHIP

---

18-732 Network Security, Carnegie Mellon University, Spring 2021  
18-330 Introduction to Computer Security, Carnegie Mellon University, Fall 2018

## EXTRA-CURRICULAR ACTIVITIES

---

Strategic Chair of the CMU ECE Diversity, Equity, Inclusion Committee  
Member of CMU CyLab Diversity, Equity, Inclusion (DEI) Committee. 2020-Present  
President of Pakistani Student Association, CMU, 2019  
Volunteer work in IRUSA, LUMS Community Service Society and an NGO named FAIDA