Phuong Cao

U.S. Permanent Resident

Research Scientist, National Center for Supercomputing Applications (NCSA) at University of Illinois Urbana Champaign
Trusted CI Fellow, National Science Foundation (NSF) Cybersecurity Center of Excellence (Trusted CI)

SUMMARY

Experienced Principal Investigator focused on building resilient and secure supercomputing systems resistant to catastrophic failures and cyber-attacks. Possesses broad expertise in real-world security, including DDoS mitigation, virus reverse engineering, post-quantum cryptography, and AI-driven malware analysis.

EDUCATION

Ph.D. in Electrical & Computer Engineering; M.S. in Computer Science	**University of Illinois at Urbana-Champaign**
B.S. in Computer Science	**Hanoi University of Science and Technology**

RESEARCH AGENDA: RESILIENCY AND SECURITY OF SUPERCOMPUTERS (HPC) SYSTEMS

Building resilient and secure infrastructure for emerging architecture such as hybrid HPC-Quantum Computing:

1. Design of provable and runtime verification techniques using Z3/Dafny for federated authentication protocols
2. Deployment of continuous attack preemption using Factor Graphs (OpenGM/Pytorch) on Teracore network
3. Validation of reliable, secure, quantum-resistant, and highly available AI/HPC/supercomputing scientific applications.

SUMMARY

Publications	20+ peer-reviewed papers in top conferences as lead author and PI. IEEE Quantum Computing and Engineering, USENIX Security/NSDI, IEEE S&P Magazine IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), Supercomputing
Awards	**Best Paper Award** at IEEE DSN, **Art of HPC and Doctoral Showcase** at SC (Supercomputing), **Best Hackathons** at Salesforce.com and Box.com, **Trusted CI Fellow** with NSF
Funding	Three grants with **$1,599,678** awarded as PI and Co-PI with federal agencies and industry partners **NSF** CISE and OAC, **IBM-Illinois Discovery Accelerator** Institute
Impact	Curated Petabytes of security and resiliency data on supercomputers (Blue Waters, Delta) and NSF testbed (FABRIC) for open-science research on Globus Preemption of cyber-attacks and recovering from outages in the U.S. HPC cyberinfrastructure
Services	Proposal Review Panels (NSF, DOE); Journals & Special Issue Editor. NSF; Frontiers; TDSC, TIFS, DSN, BigData, SIGCOMM, Quantum Computing and Engineering
Teaching	Graduate-level **AI, data science, statistics, dependable systems and computer security courses** at Coordinated Science Lab (CSL) as guest lecturer and TAs
Outreach	Mentor for CyberCorps Scholarship for Service (SFS) students (recognized as an **outstanding mentor** for a Fiddler Innovation Fellowship awardee)
Work Authorization	U.S. Permanent Resident via EB1-A (Extraordinary Ability) – *Vietnamese* national.

APPOINTMENTS

2020–	*Research Scientist* and Cybersecurity Specialist	**National Center for Supercomputing Applications**
2019	*Research Intern*, Research in Software Engineering (RiSE), formal verification	**Microsoft Research**
2016	*Research Intern*, IBM zSystems mainframes and Watson Health	**IBM Research**
2014	*Engineering Intern*, DDoS detection at Layer-7 in Content Delivery Networks	**LinkedIn & Akamai**
2011	*Visiting scholar*, High-Performance Computing Lab with Professor Jong Kim	**POSTECH University**

CONTACT

pcao3@illinois.edu
https://go.illinois.edu/pcao3
1205 W. Clark St., 3006B
Urbana, IL, 61801

REFERENCES

William Kramer, Blue Waters PI, Research Professor at UIUC

Anita Nikolich, Director of Research and Technology, iSchool, UIUC

Gang Wang, Associate Professor, Siebel School of Computing and Data Science, UIUC

Ravishankar Iyer, George and Ann Fisher Distinguished Professor, ECE, UIUC

GRANTS

Awarded as lead PI and Co-PI. Total $1,5999,678 **Role**

2025-2027 **EAGER: Unmasking HPC Abuse: AI Graph Inference from Scheduling Metadata** **PI**
NSF Office of the Chief of Research Security Strategy and Policy (CRSP) #2537355 $274,654

2025-2028 **AICyberLake: Live Evaluations of Real-World Security Data Lake from National AI-Cyberinfrastructure** **PI**
NSF Cybersecurity Innovation for Cyberinfrastructure (CICI) #2530738 $600,000

2023-2025 **ResiliANT AIOps: Foundation-Model-Driven Resilience for Cloud Computing** **Co-PI**
International Business Machines – IBM-Illinois Discovery Accelerator Institute $699,679

2024-2026 **Quantum-Resistant Cryptography in Supercomputing Scientific Applications** **PI**
NSF Office of Advanced Cyberinfrastructure (OAC) Award #2430244 $200,000

2023-2025 **FMitF: Bringing Verification-Aware Languages and Federated Authentication to Enable Secure Computing for Scientific Communities** **PI**
NSF Formal Methods in the Field (FMitF); CISE/CCF Award #2319190 $99,999

Awards with significant contributions in preparation and execution **Role**

2023 **Mid-Scale RI-1: FABRIC: Adaptive Programmable Research Infrastructure for Computer Science and Science Applications** Security Engineer
NSF Mid-Scale RI-1 (CNS) # 1935966

2021 **PPoSS: Inflight Analytics to Control Large-Scale Heterogeneous Systems** Personnel
NSF Principles and Practice of Scalable Systems (PPoSS) #2029049

Awards with UIUC and International Partners **Role**

2024-2029 **Enhancing Precision Digital Pathology with an AI-accelerated Supercomputers** **Co-PI**

2024-2029 **Accelerating Patient Rehabilitation via Wearable Filament Sensor Networks** **Co-PI**
VinUni-Illinois Smart Health Center Five Funded PhD students and one Postdoc

HONORS AND AWARDS

2024 **Art of High Performance Computing (HPC) exhibit**, IEEE/ACM Supercomputing Artwork Atlanta, GA

2024 **Outstanding Mentors**, Students Pushing INnovation (SPIN) with Fiddler Innovation Endowment awardee link

2023 **Trusted Cyber Infrastructure (CI) Fellows**, NSF Cybersecurity Center of Excellence link

2023 **Doctoral Showcase**, IEEE/ACM Supercomputing Denver, CO

2014 **Best Paper Award** - IEEE/IFIP Dependable Systems and Networks (DSN) Atlanta, GA

2014 **$10,000 Hackathon prize**, Salesforce $1 Million Hackathon ($10^{th}$ place) San Francisco, CA

2012 **Best Use of the APIs**, Box.com Hackathon Redwood City, CA

2011 **Vietnam Education Foundation (VEF) Fellowship** nomination (top 45 Vietnamese students) Hanoi, Vietnam

2009 **American Chamber of Commerce Scholar**, Hanoi chapter Hanoi, Vietnam

2006 **FPT Young Talents Technology Centre** (FYT), 8^{th} cohort Hanoi, Vietnam

SELECTED PUBLICATIONS

2025 **Characterizing GPU Resilience and Impact on AI/HPC Systems**
Shengkun Cui, Archit Patke, Ziheng Chen, Aditya Ranjan, Hung Nguyen, **Phuong Cao**, Saurabh Jha, Brett Bode, Gregory Bauer, Chandra Narayanaswami, Daby Sow, Catello Di Martino, Zbigniew Kalbarczyk, Ravishankar Iyer
ACM/IEEE Supercomputing'25 arXiv:2503.11901 St. Louis, MO

2025 **Dependable Classical-Quantum Computer Systems Engineering**
Edoardo Giusto, Santiago Nuñez-Corrales, **Phuong Cao**, Alessandro Cilardo, Ravishankar K Iyer, Weiwen Jiang, Paolo Rech, Flavio Vella, Bartolomeo Montrucchio, Samudra Dasgupta, Travis S Humble
https://arxiv.org/abs/2408.10484 Frontiers Special Issue

2024 **Post-Quantum Cryptography (PQC) Network Instrument: Measuring PQC Adoption Rates and Identifying Migration Pathways**
Jakub Sowa, Bach Hoang, Advaith Yeluru, Steven Qie, Anita Nikolich, Ravishankar Iyer, **Phuong Cao**
IEEE International Conference on Quantum Computing and Engineering (QCE)
DOI: 10.1109/QCE60285.2024.00213 Montreal, Canada

2024 **True Attacks, Attack Attempts, or Benign Triggers?**
An Empirical Measurement of Network Alerts in a Security Operations Center
Limin Yang, Zhi Chen, Chenkai Wang, Zhenning Zhang, Sushruth Booma, Constantin Adam, Alex Withers, **Phuong Cao**, Zbigniew Kalbarczyk, Ravishankar Iyer, Gang Wang.
Proceedings of the 33rd *USENIX Security* Symposium
DOI: 10.5555/3698900.3698986 Philadelphia, PA

2023 **stealthML: Data-driven Malware for Stealthy Data Exfiltration**
Keywhan Chung, **Phuong Cao**, Zbigniew Kalbarczyk, Ravishankar Iyer.
In the *IEEE International Conference on Cyber Security and Resilience (CSR)*
DOI: 10.1109/CSR57506.2023.10224946 Venice, Italy

2020 **Investigating Root Causes of Authentication Failures Using a SAML and OIDC Observatory**
Jim Basney, **Phuong Cao**, Terry Fleury
In *the 6th IEEE International Conference on Dependability in Sensor, Cloud, and Big Data Systems and Applications (DependSys)*
10.1109/DependSys51298.2020.00026 Virtual

2019 **Continuous Auditing of SSH-Servers To Mitigate Brute-Force Attacks**
Phuong Cao, Yuming Wu, Subho Banerjee, Justin Azoff, Alex Withers, Zbigniew Kalbarczyk, Ravishankar Iyer
In *the 16th USENIX Symposium on Networked Systems Design and Implementation (NSDI)*
DOI: 10.1109/DependSys51298.2020.00026 Boston, MA

2016 **SVAuth: A Single-Sign-On Integration Solution with Runtime Verification**
Shuo Chen, Matt McCutchen, **Phuong Cao**, Shaz Qadeer, and Ravishankar Iyer
In *the 17th International Conference on Runtime Verification (RV)*
PDF Madrid, Spain

2014 **Preemptive intrusion detection: theoretical framework and real-world measurements**
Phuong Cao, Eric Badger, Adam Slagell, Zbigniew Kalbarczyk, Ravishankar Iyer
In *the Symposium and Bootcamp on the Science of Security (HotSOS)*
PDF Raleigh, NC

2013 **Security Monitoring for Virtual Machines Using Hardware Architectural Invariants**
Cuong Pham, Zachary Estrada, **Phuong Cao**, Zbigniew Kalbarczyk, Ravishankar Iyer
Best Paper Award. In *the 44th IEEE Conference on Dependable Systems and Networks (DSN)*
PDF Atlanta, GA

SUBMITTED MANUSCRIPTS

2025 **Building Machine Learning Challenges for Anomaly Detection in Science**
Campolongo, Elizabeth G., Yuan-Tang Chou, Ekaterina Govorkova, Wahid Bhimji, Wei-Lun Chao, Chris Harris, Shih-Chieh Hsu et al. (**Phuong Cao** Endorser) Submitted to Nature Communications
https://arxiv.org/abs/2503.02112

2025 **Dynamic Factor Graphs for Attack Preemption**
Phuong Cao, Zbigniew Kalbarczyk, Ravishankar Iyer Submitted to IEEE TDSC.

CONTRIBUTED BOOK CHAPTERS

2024 **Dependable Computing: Design and Assessment**, ISBN: 978-1-118-70944-3 IEEE Wiley

2023 **Multimodal AI in Healthcare**, ISBN: 978-3-031-14771-5 Springer

2018 **Assured Cloud Computing**, ISBN: 978-1-119-42863-3 IEEE Wiley

MAGAZINE ARTICLES

2014 **Building Reliable and Secure Virtual Machines Using Architectural Invariants**
Cuong Pham, Zachary Estrada, **Phuong Cao**, Zbigniew Kalbarczyk, Ravishankar Iyer
In *the IEEE Security & Privacy (S&P) Magazine*

WORKSHOPS

2024 **Security Testbed for Preempting Attacks against Supercomputing Infrastructure**
Phuong Cao, Zbigniew Kalbarczyk, Ravishankar Iyer
Secure-HPC Workshop organized by NIST and PNLL, co-located with IEEE/ACM Supercomputing Atlanta, GA

2024 **Auditing Network Security Attacks in Jupyter Notebooks**
Phuong Cao
INDIS Workshop, co-located with IEEE/ACM Supercomputing Atlanta, GA

2023 **Taxonomy of Fingerprinting Techniques for Evaluation of Smart Grid Honeypot Realism**
Vanessa Tay Sin Yee, Xinran Li, Daisuke Mashima, Bennet Ng, **Phuong Cao**,
Zbigniew Kalbarczyk, Ravishankar Iyer.
Workshop on Testbed and Digital Twin for Smart Grids, *IEEE SmartGridComm* Glasgow, Scotland

2023 **Post-Quantum Cyberinfrastructure Security Readiness: Risks, Measures and Prospects**
Phuong Cao, Bach Hoang, Santiago Nunez-Corrales.
In *Basic Research Needs in Quantum Computing and Networking*,
Department of Energy's Office of Advanced Scientific Computing Research Gaithersburg, MD

2022 **Predicting COVID-19 Disease Progression with A Factor Graph-based Model**
Yurui Cao, **Phuong Cao**, Haotian Chen, Karl M. Kochendorfer,
Andrew B. Trotter, William L. Galanter, Paul M. Arnold, Ravishankar Iyer.
In *Association for the Advancement of Artificial Intelligence (AAAI) Health Intelligence* Workshop Virtual

2020 **Mining threat intelligence from billion-scale SSH brute-force attacks**
Yuming Wu, **Phuong Cao**, Alexander Withers, Zbigniew Kalbarczyk, Ravishankar Iyer.
In *Network and Distributed System Security (NDSS) Symposium* Workshop
PDF San Diego, CA

2012 **Toward a high availability cloud: Techniques and challenges**
Cuong Pham, **Phuong Cao**, Zbigniew Kalbarczyk, and Ravishankar Iyer
In *the 42nd IEEE International Conference on Dependable Systems and Networks (DSN)* Workshop Boston, MA

COURSES: SYLLABUS DESIGNS, MACHINE PROBLEMS, AND LECTURES

University of Illinois at Urbana-Champaign

2023	**ECE 598 RKI: Trustworthy AI Systems**	Guest Lecturer
2022	**ECE 471: Data Science Analytics using Probabilistic Graphical Models**	Machine Problem designer
2021	**ECE 542 / CS 536: Design of Fault Tolerant Digital Systems**	Guest Lecturer
2020	**ECE 598 RKI: Dependable AI Systems**	Machine Problem designer
2020	**CS 498 : Data Science & Analytics**	Machine Problem designer
2019	**ECE 542 / CS 536: Design of Fault Tolerant Digital Systems**	Teaching Assistant
2018	**CS 461: Computer Security**	Teaching Assistant
2017	**CS 461: Computer Security**	Teaching Assistant
2017	**ECE 313: Probability and Statistics**	Teaching Assistant

TUTORIALS, TALKS AND LECTURES

2025 **Quantitative Risk Assessment for Post Quantum Cryptography**
Joint Laboratory for Extreme Scale Computing (JLESC), Argonne National Laboratory Lemont, IL

2025 **Quantitative Risk Assessment for Post Quantum Cryptography**
5^{th} NIST Secure HPC Workshop Gaithersburg, MD

2025 **Measuring Quantum Resistant Cryptography**
Hot Topics in the Science of Security Symposium (HotSoS) Virtual, hosted by NSA

2024 **Jupyter Notebooks Security**
Supercomputing Atlanta, GA

2024 **Secure HPC Software Construction, Communication, and Computation**
Illinois Cyber Security Scholars Program (ICSSP) Urbana, IL

2024 **Security Log Analysis** Tutorial
NSF Cybersecurity Summit at Carnegie Mellon University (CMU) Pittsburg, PA

2024 **Post Quantum Cryptography Adoption Rate**
NIST HPC Security Working Group Virtual

2024 **Secure HPC Software Construction, Communication, and Computation**
4^{th} High-Performance Computing Security Workshop, Wichita State University Wichita, KS

2024 **Post Quantum Cryptography Migration for HPC**
National Center for Supercomputing Applications
Quantum Computing Interest Group Monthly Meeting Urbana, IL

2023 **Plenary Session | NSF Trusted CI Fellows Panel**
Lawrence Berkeley National Lab Berkeley, CA

2023 **Secure Infrastructure for Health Analytics**
National University of Singapore (NUS), Illinois Advanced Research Center (Illinois ARCS) Singapore

2023 **Evolution of malicious software in the machine learning domain**
ECE 598RKI: Dependable AI Systems Urbana, IL

2023 **Towards Reliable and Robust Generative Models in Systems Domain**
Winter School on Cyber Security – Hanoi University of Science & Technology Hanoi, Vietnam

2023 **Innovations in Health Analytics and Systems: An Illinois Engineering and Mayo Clinic Partnership**
VinUni-Illinois Smart Health Center Hanoi, Vietnam

2023 **Expert-guided Foundational Model for Preemptive Attack Detection**
Hanoi University of Science and Technology (Bach Khoa), Hanoi, Vietnam

2023 **Secure Infrastructure for Health Analytics**
VinMec hospital Hanoi, Vietnam

2022 **Factor graphs & Belief Propagations**
ECE 471: Data Science Analytics using Probabilistic Graphical Models Urbana, IL

2021 **Bot vs. Human: Statistical analysis of honeypot logs**
CS 536: Design of Fault Tolerant Digital Systems Urbana, IL

2020 **Replay of security attacks in a production testbed**
CS 498 : Data Science & Analytics Urbana, IL

2019 **Continuous Auditing of SSH-Servers To Mitigate Brute-Force Attacks**
Microsoft Research, Cryptography, Security, and Privacy (CRYSP) Bellevue, WA

CONFERENCE ACTIVITIES

2024 **Bringing Verification-Aware Languages and Federated Authentication to Enable Secure Computing for Scientific Communities** *Poster*
NSF Formal Methods in the Field (FMitF) PI Meeting Iowa City, IA

2024 **Verifying Critical Authentication Systems in Research Infrastructure** *Posters*
NSF Research Infrastructure Workshop Phoenix, AZ

2023 **Enriching Energy Systems Threat Intelligence Foundation-Model-driven SmartGrid Honeypot** *Industry Advisory Board Meeting*
Center for Infrastructure Trustworthiness in Energy Systems Chicago, IL

2023 **Preemptive Intrusion Detection: Real-world Measurements, Bayesian-based detection, and AI-driven countermeasures** *Doctoral Showcase*
International Conference for High-Performance Computing, Networking, Storage, and Analysis (SC) *Denver, CO*

2023 **Security and Resiliency Challenges in Hybrid HPC-QC (High-Performance-Supercomputer-Quantum-Computing)** *Poster*
NSF Cybersecurity Summit, Lawrence Berkeley National Laboratory Berkeley, CA

2023 **Security Log Analysis – Ransomware encounters in the wild** *Tutorial (Interactive) Session*
NSF Cybersecurity Summit, Lawrence Berkeley National Laboratory Berkeley, CA

2023 **Foundational Resiliency Model on the Blue Waters Petascale Supercomputer** *Presentation*
DEPEND group research retreat Urbana, IL

2023 **Post-Quantum Cryptography (PQC) Adoption Measured at the National Center for Supercomputing Applications (NCSA)** *Poster*
Sandia-UIUC Mini-Conference Urbana, IL

2023 **quAPL-V: Formal Verification in an Array Programming Language-based quantum library** *Poster*
Sandia-UIUC and NCSA Industry Conference Urbana, IL

2023 **stealthML: Data-driven Malware for Stealthy Data Exfiltration** *Presentation*
IEEE International Conference on Cyber Security and Resilience Venice, Italy

2023 **Towards Reliable and Robust Generative Models in Clinical and Systems Domain** *Presentation*
Mayo Clinic Rochester, MN

2023 **Post-Quantum Cryptography (PQC) Adoption Measured at the National Center for Supercomputing Applications (NCSA)** *Poster*
Illinois Quantum Information Science & Technology Center (IQUIST) All-Hands Meeting Urbana, IL

2023 **Applications of eBPFs in bastion host auditing** *Demo*
NSF Campus Cyberinfrastructure (CC) PI Meeting and FABRIC Workshop* Columbus, OH

2023 **Ransomware Honeypot** *Presentation*
U.S. Army Corps of Engineers (USACE) R&D Day Urbana, IL

2023	**Verifying quAPL: an APL-based quantum programming library** *STEM Career Exploration and Research Symposium*	*Presentation* Urbana, IL
2023	**Formal Verification of SciTokens** *NCSA Student Research Symposium*	*Presentation* Urbana, IL
2022	**A data anonymization proxy for interactive log analyses** *NSF Cybersecurity Summit*	*Presentation* Bloomington, IN
2022	**Predicting ICU Admissions for Hospitalized COVID-19 Patients with a Factor Graph-based Model** *Association for the Advancement of Artificial Intelligence (AAAI)-22 Workshop*	*Presentation* Vancouver, BC, Canada
2021	**Investigating Remote Desktop Protocols attacks using the Zeek observatory at UIUC/NCSA** *Zeek Week*	*Presentation* Virtual
2021	**Ransomware Honeypot** *NSF Cybersecurity Summit* and *FABRIC Knit Workshop*	*Presentation* Chicago, IL
2021	**Real-time & Interpretable Inference for COVID-19 Disease Progression using Factor Graph Models** *Center for Computational Biotechnology and Genomic Medicine (CCBGM)*	*Poster* Urbana, IL
2020	**Investigating Root Causes of Authentication Failures Using a SAML and OIDC Observatory** *IEEE DependSys*	*Presentation* Fiji - Virtual
2020	**Analysis of remote desktop protocol attacks targeting scientific computing infrastructure during the COVID19 pandemic** *Fourth Workshop on Trustworthy Scientific Cyberinfrastructure (TrustedCI@PEARC20)*,	*Presentation* Virtual
2020	**Mining Threat Intelligence from Billion-scale SSH Brute-Force Attacks** *Network and Distributed System Security (NDSS) Symposium*	*Poster* San Diego, CA
2019	**Continuous Auditing of SSH-Servers To Mitigate Brute-Force Attacks** *National University of Singapore*	*Presentation* Virtual
2019	**Formal Verification of Smart Contracts** *Microsoft Research*	*Presentation* Redmond, WA
2019	**TRACTION: an infrastructure for trusted alert sharing and collaborative mitigation** *ACM HotSoS*	*Poster* Nashville, TN
2019	**Continuous Auditing of SSH-Servers To Mitigate Brute-Force Attacks** *USENIX Symposium on Networked Systems Design and Implementation (NSDI)*	*Presentation* Boston, MA
2019	**Continuous Auditing of SSH-Servers To Mitigate Brute-Force Attacks** *Security and Privacy Research at Illinois*	*Presentation* Urbana, IL.
2018	**A security testbed for capturing, replaying, and auditing attacks** *ACM Internet Measurement Conference (IMC)*	*Poster* Boston, MA
2017	**Learning Factor Graphs for Preempting Multi-State Attacks in Cloud Infrastructure** *Symposium and Bootcamp on the Science of Security (HotSoS 2017)*	*Poster* Hanover, MD
2017	**A Real-world Testbed for Assessing Security of Electronic Health Data Sharing** *Center for Computational Biotechnology and Genomic Medicine (CCBGM)*	*Poster* Urbana, IL
2017	**Self-Verifying Authentication: Safer Integrations of Single-Sign-On Services** *Blackhat Europe*	*Presentation* London, United Kingdom
2017	**SVAuth–A Single-Sign-On Integration Solution with Runtime Verification** *International Conference on Runtime Verification (RV)*	*Presentation* Seattle, WA
2017	**An Ethical Hacking Framework for Assessing Security of Cloud Infrastructure** *IBM IEEE CAS/EDS – AI Compute Symposium*	*Poster* Yorktown Heights, NY
2016	**An Ethical Hacking Framework for Assessing Security of Cloud Infrastructure** *IBM Research*	*Presentation* Austin, TX
2016	**Personalized password guessing: a new security threat** *ACM HotSoS*	*Poster* Pittsburgh, PA
2015	**Towards an unified security testbed and security analytics framework** *ACM HotSoS*	*Poster* Urbana, IL
2015	**Towards an unified security testbed and security analytics framework** *Supercomputing (SC)*	*Demo* Austin, TX
2014	**Reliability and security monitoring of virtual machines using hardware architectural invariants** *IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*	*Presentation* Atlanta, GA
2014	**Application-layer Denial of Service Attacks** *LinkedIn*	*Presentation* Mountain View, CA

2014	**Preemptive Intrusion Detection** *ACM HotSoS*	*Presentation* Raleigh, NC
2014	**Preemptive Intrusion Detection** *Information Trust Institute (ITI)*	*Presentation* Urbana, IL
2013	**Factor Graphs modeling in Anti Money Laundering** *IBM Research*	*Presentation* Yorktown Heights, NY
2012	**Applications of Machine Learning in Layer-7 Slow DDoS Detection** *Akamai*	*Presentation* San Mateo, CA

ACADEMIC SERVICES

Journal Editor

2024 **Frontiers**: *Realizing Quantum Utility: Grand Challenges of Secure & Trustworthy Quantum Computing*

Workshop Organizer

2024 First Workshop on Dependability Challenges in Hybrid Classical-Quantum Computing Systems
Co-located with QCE24

2024 Dependable Architectures for HPC and Quantum Systems
Joint High-Performance Quantum Dependability Working group: Fermi National Accelerator Laboratory, Oak Ridge National Laboratory, UIUC (IQUIST, NCSA, CSL/ECE), University of Naples Federico II

GRANT AND AWARD REVIEWERS

Grant and Award Reviewers

2025 Proposal Reviewer, Department of Energy (DOE)

2024-2025 Panelist, National Science Foundation (NSF)

2022 C3.ai Digital Transformation Institute

Judges

2023-2024 Technical Judge, Hack Illinois

2023-2024 Mentor, NCSA's SPIN (Students Pushing Innovation) – an NSF REU site.

2019 Judge, Pulse Hardware Competition, ECE Illinois

2022 Illinois CS & ECE graduate admission

2012-2019 Chair & Organizer, DEPEND group research retreat

Technical Conference Program Committee (TPC) Member

2025 Foundations Of Reliable Classical-quantum Engineering, IEEE/IFIP DSN 2025

2024-2025 Program Committee Member, IEEE International Conference on Quantum Computing and Engineering (QCE)
Quantum Networking track link

2023-2024 Program Committee Member, US Research Software Engineer Association (US-RSE)

2019 ACM Internet Measurement Conference (IMC), Shadow Program Committee

Conference Chairs

2024 Program Co-Chair, 54th Annual IEEE/IFIP International Conference on Dependable Systems and Networks, Industry Track

Journal peer reviews (verified): Clarivate Web of Science

2024,2025 IEEE Transactions on Information Forensics and Security (IEEE TIFS)

2024 Journal of Open Source Software (JOSS)

2018 IEEE Transactions on Dependable and Secure Computing (IEEE TDSC)

Conference reviewers

IEEE International Symposium on On-Line Testing and Robust System Design (IEEE IOTLS)

ACM Special Interest Group on Data Communication (ACM SIGCOMM)

IEEE International Conference on Dependable Systems and Networks (IEEE DSN)

IEEE International Conference on Cloud Computing (IEEE CLOUD)

IEEE International Conference on Big Data (IEEE BigData)

IEEE International Symposium on On-Line Testing & Robust System Design (IOLTS)

NeurIPS

OUTREACH ACTIVITIES

Jul 2024	**Secure Health Analytics in Supercomputing Environment** *VinUni-Illinois Summer School for Pre-doctoral Students*	Hanoi, Vietnam
Oct 2024	**National Petascale Computing Facility** tour for UIUC Sysnet and SPRAI students	Champaign, IL
Apr 2024	**Engineering Open House https://eohillinois.org/**, NCSA,	Urbana, IL.
Nov 2023	**Federated Authentication explained for K12 students**, Carrie Busey Elementary School	Savoy, IL
Oct 2023	**National Petascale Computing Facility** tour for VinUni-Illinois visiting scholars and SPRAI	Champaign, IL
June 2023	**National Petascale Computing Facility** tour for Students Pushing Innovation (SPIN) students	Champaign, IL

STUDENTS MENTORED AND ADVISED

Exchange students

Thibaut Probst → Airbus
Chi Phan → VinUni
Hung Nguyen → VinUni → UIUC → Argonne National Lab
Cuong, Nguyen Tien → Singapore University of Technolgy and Design (SUTD)

Undergraduates

Jakub Sowa → NSF CyberCorps Scholarship for Services (current); Awarded **Fiddler Innovation** Fellowship.
Seoung Kyun Kim → National Renewable Energy Laboratory (NREL)
Surya Bakshi → Offchain Labs
Binfeng Yuan → Amazon
Satvik Kulkarni → IBM
Advay Kadam → NCSA
Bach Hoang → NCSA

Master students

Eric Badgers → Yahoo!

PhD students

Yurui Cao
Yuming Wu

MEMBERSHIPS

Present	**Institute of Electrical and Electronics Engineers (IEEE)**	Member
Present	**Quantum Community, Institute of Electrical and Electronics Engineers (IEEE)**	Member

PUBLICLY AVAILABLE CODE AND DATA RELEASES

2023	Blue Waters **security** and resiliency data (approximately one Petabyte)	Globus
2019	SSH-auditor	URL
2019	SSH Honeypot Data (complete 15B SSH attack attempts available on request)	URL
2018	SVAuth: Self-verifying single-sign-on solutions	URL
2017	Timemachine – reproducible vulnerabilities in Debian-based docker container.	Docker Hub; Github
2000-2023	Longitudinal data of NCSA security incidents (sys logs, reports, and Zeek logs)	Available upon request

PRESS

2025	**HPCWire**, *NCSA Awards 17 Students Fiddler Innovation Fellowships*	URL
2024	**HPCWire, Quantum Zeitgeist, Quantum Insider**, *NCSA's New Project Paves Path to Quantum-Resistant Cyberinfrastructure in Scientific Computing*	URL
2019	**HPCWire, ECE Illinois, NCSA**, *Illinois Researchers Sweeten Honeypot to Catch, Blacklist Hackers*	URL

ADDITIONAL INFORMATION

References

Alexander Withers, *Deputy Chief Information Security Officer*, Department of Energy's Energy Sciences Network (ESnet)
Jim Basney, *Director and PI of Trusted CI*, NSF Cybersecurity Center of Excellence.
Minh Do, *Thomas and Margaret Huang Endowed Professor*, University of Illinois, Urbana-Champaign.
William Kramer, *Executive Director of the Illinois New Frontiers Initiative and Blue Waters Director*, NCSA
Additional references are available upon requests.

Degree

PhD degree is expected to be conferred before the start date.

MISC

Misc. travel grants

- **NSF Cybersecurity Summit, Supercomputing, HotSoS, ACM IMC, NSF CC* PI meetings**

PAST APPOINTMENTS

2010	*Intern*, High Performance Computing	**Pohang University of Science and Technology (POSTECH)**
2010	*Research Engineer*, Faceted Search	**Vinagame (VNG)**
2006-09	*Security Intern*, Reverse Engineering Computer Viruses	**Bach Khoa Anti-Virus (BKAV)**