

Rakesh Podder

Email: rakeshpodder3@gmail.com | Website: [Rakesh Podder](#) | LinkedIn: [Rakesh Podder](#)
CSU Email: rakesh.podder@colostate.edu Mobile: +1 (970)732-8524 | Google Scholar: [Rakesh Podder](#)

Biography

I am a Ph.D. candidate in Computer Science at Colorado State University, advised by Prof. Indrajit Ray. My research develops AI-planning-based frameworks for the security and resiliency analysis of cyber-physical systems, centered on three connected contributions: attack-connectivity graph analysis (SPEAR and i-EXAM), unified Resiliency and Safety Graph frameworks for modeling cascading IT-OT failures, and SERA, a re-programmable simulation testbed for explainable resiliency analysis. Alongside this work, I develop CAPE, a context-aware vulnerability prioritization engine, as an independent research line. From 2024 to 2026, I served as a Foreign Research Scientist at the National Institute of Standards and Technology (NIST), collaborating with Irena Bojanova on the Bugs Framework to formalize the classification of security bugs, CVEs, and CWEs. My research has been supported by the Office of Naval Research, the National Science Foundation, and the Department of Energy, and recognized with *Best Paper awards* at *IEEE TPS-ISA 2024* and *IEEE QRS 2024*. Alongside research, I teach and mentor at CSU as a graduate teaching assistant and research mentor, designing hands-on security labs and lecturing independently when called on. Before CSU, I completed an M.E. in Electrical Engineering at Jadavpur University (Gold Medalist) and a B.Tech at the Indian Institute of Technology, Patna, followed by industry experience at Infosys and Cognizant.

Career Objective

I am seeking a tenure-track Assistant Professor position where I can build an independent, externally funded research program that extends my work in planning-based cyber-physical system security into hardware and firmware security — building on my Electrical Engineering background (M.E., Jadavpur University; B.Tech, IIT Patna) and my existing work on Hardware Root of Trust and firmware attestation (S-RFUP, PIT, CoDICE) — alongside critical infrastructure and software supply chain security, and to translate that research into hands-on, project-based coursework. Having contributed to funded projects supported by ONR, NSF, and DOE as a graduate researcher, I am positioned to pursue independent grant funding early in a faculty career. My approach to teaching is grounded in active-learning methods: I designed penetration-testing and reverse-engineering labs for CS557 and led the CSU Cybersecurity Summer Camp for three consecutive years, and I look forward to building a similarly hands-on curriculum in systems and hardware security while mentoring the next generation of researchers and professionals in the field.

Research Interests

Cyber-Physical System Resiliency • Attack Graphs Modeling • Vulnerability Analysis • AI Planning • Firmware Security • Hardware Security • Hardware Root of Trust (HROt) • Formal Security Verification • Large Language Models (LLMs) • Adversarial Machine Learning • Explainable AI (XAI) • Threat Intelligence • Intrusion Detection Network Security • IoT Security • Financial Fraud Detection • Graph-theoretic Security Analysis • AI Ethics • Responsible AI • Critical Infrastructure Security • Software Bill of Materials (SBOM) • Supply Chain Security • Cyber Security Education

Education and Qualifications

2022 – present

Ph.D. Candidate

Computer Science Department

Colorado State University, Fort Collins, CO, USA 80521

CGPA: 4.00/4.00

2022 – 2025	Master of Science (Thesis) Computer Science Department Colorado State University, Fort Collins, CO, USA CGPA: 4.00/4.00 <i>Thesis: Preventing Malicious Modifications to Firmware Using Hardware Root of Trust (HRoT)</i>
2018 – 2020	Master of Engineering (Thesis) Electrical Engineering Department Jadavpur University, Kolkata, West Bengal, India CGPA: 9.11/10 (Gold Medalist) <i>Thesis: Data Security of IoT Enabled Autonomous Robots from the Perspective of its Various Controlled Actions</i>
2013 – 2017	Bachelor of Technology Electrical Engineering Department Indian Institute of Technology, Patna, Bihar, India CGPA: 7.5/10 <i>Dissertation: Low Cost Signal Generator</i>

Publications

Peer-Reviewed Conference

1. **R. Podder**, F. G. Arellano and I. Ray, "Hidden Amplifiers: Cross-Level Risk in Software Supply Chains," in *Proceedings of the 42nd International Conference on Software Maintenance and Evolution (ICSME)*, 2026. [Accepted].
2. **R. Podder** and I. Ray, "SERA – An AI Driven Re-Programmable Simulation Environment for Explainable Resiliency Analysis in Cyber-Physical Systems," in *Proceedings of the 6th ACM Workshop on Secure and Trustworthy Cyber-Physical Systems (SaT-CPS '26)*, Frankfurt am Main, Germany, June 23–25, 2026. 10.1145/3806008.3811708
3. **R. Podder**, W. Ganim, S. Sreedharan, I. Ray, and I. Ray, "i-EXAM: Instructable and Explainable Attack Connectivity Graph Modeler," in *Proceedings of the International Conference on Automated Planning and Scheduling (ICAPS '26)*, 2026. (*Demo Paper.)
4. **R. Podder**, J. Simental, E. Azizli, B. Mantha and I. Ray, "CoDICE: Roll the DICE for Firmware Attestation," in *Proceedings of 2025 IEEE 7th International Conference on Trust, Privacy and Security in Intelligent Systems, and Applications (TPS-ISA)*, Pittsburgh, PA, USA, 2025, pp. 183-196. 10.1109/TPS-ISA67132.2025.00028
5. T. Rhaimi, H. Aghayarzadeh, **R. Podder** and I. Ray, "Formal Specification and Verification of Protection in Transit (PIT) Protocol Using UPPAAL." in *Proceedings of 2025 22nd Annual International Conference on Privacy, Security, and Trust (PST)*. Fredericton, NB, Canada, 2025, pp. 1-6. 10.1109/PST65910.2025.11268865
6. **R. Podder** T. Caglar, S. K. Bashir, S. Sreedharan, I. Ray, and I. Ray, "SPEAR: Security Posture Evaluation using AI Planner-Reasoning on Attack-Connectivity Hypergraphs." in *Proceedings of the 30th ACM Symposium on Access Control Models and Technologies (SACMAT '25)*. Association for Computing Machinery, New York, NY, USA, 62–73. 10.1145/3734436.3734451
7. R. Talukdar, **R. Podder**, and I. Ray, "VKG2AG : Generating Automated Knowledge-Enriched Attack Graph (AG) from Vulnerability Knowledge Graph (VKG)." in *Proceedings of the 22nd International Conference on Security and Cryptography (SECRYPT 2025)*. SciTePress, pp. 420-428. 10.5220/0013526700003979
8. **R. Podder**, T. Rios, I. Ray, P. Raman, and S. Righi, "S-RFUP: Secure Remote Firmware Update Protocol." in *Proceedings of the International Conference on Information Systems Security (ICISS 2024)*.

Lecture Notes in Computer Science, Cham, Springer Nature Switzerland, vol 15416, pp. 42-62. 10.1007/978-3-031-80020-7_3

9. S. K. Bashir*, **R. Podder***, S. Sreedharan, I. Ray and I. Ray, "Resiliency Graphs: Modelling the Interplay between Cyber Attacks and System Failures through AI Planning," in *Proceedings of the 2024 IEEE 6th International Conference on Trust, Privacy and Security in Intelligent Systems, and Applications (TPS-ISA)*, Washington, DC, USA, 2024, pp. 292-302. (***Equal contribution.**) 10.1109/TPS-ISA62245.2024.00041 (*Best Paper Award*)
10. **R. Podder** and S. Ghosh, "Impact of White-Box Adversarial Attacks on Convolutional Neural Networks." in *Proceedings of the 2024 International Conference on Emerging Trends in Networks and Computer Communications (ETNCC)*, Windhoek, Namibia, 2024, pp. 1-9. 10.1109/ETNCC63262.2024.10767521
11. **R. Podder**, J. Sovereign, I. Ray, M. B. Santharam and S. Righi, "The PIT-Cerberus Framework: Preventing Device Tampering During Transit." in *Proceedings of the 2024 IEEE 24th International Conference on Software Quality, Reliability and Security (QRS)*, Cambridge, United Kingdom, 2024, pp. 584-595. 10.1109/QRS62785.2024.00064 (*Best Paper Award*)
12. I. Ray, S. Sreedharan, **R. Podder**, S. K. Bashir and I. Ray, "Explainable AI for Prioritizing and Deploying Defenses for Cyber-Physical System Resiliency." in *Proceedings of the 2023 5th IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA)*, Atlanta, GA, USA, 2023, pp. 184-192. 10.1109/TPS-ISA58951.2023.00032
13. **R. Podder** and R. K. Barai, "Hybrid Encryption Algorithm for the Data Security of ESP32 based IoT-enabled Robots." in *Proceedings of the 2021 Innovations in Energy Management and Renewable Resources(52042)*, Kolkata, India, 2021, pp. 1-5. 10.1109/IEMRE52042.2021.9386824

Peer-Reviewed Journal

1. **R. Podder**, M. Abdelgawad, I. Ray, I. Ray, M. Santharam, and S. Righi, "Correctness and security analysis of the protection in transit (PIT) protocol." *Journal of Systems and Software*, 230, p.112501, 2025. 10.1016/j.jss.2025.112501
2. R. Muslim, R. Delfianti, C. Harsito, S. Palaloi, N. A. Aryono, A. Y. Indrarahmana, S. R. Joshua, and **R. Podder**, "Optimizing the Integration of Wind and Solar Power for Hybrid Electrical Energy in High-Rise Building Energy Systems," *Engineered Science*, 35, p.1555, 2025. 10.30919/es1555
3. E. Rovianto, R. Delfianti, F. Minelli, C. Harsito, **R. Podder** and S. R. Joshua, "Crossflow Thermo-electric Kitchen Hood System for Enhancing Sustainable Energy in Buildings," *Civil Engineering Journal*, 12(6), 2402–2414. 10.28991/CEJ-2026-012-06-014

Peer-Reviewed Conference Abstract

1. I. Ray, **R. Podder**, S. Sreedharan, I. Ray, and S. K. Bashir, "iEXAM: AI-Driven Cyber Security with Explainability." in *2026 CAE Cybersecurity Community Symposium*, Pittsburgh, Pennsylvania, 2026, pp. 73. [Abstract Link](#)
2. I. Ray, S. K. Bashir, **R. Podder**, S. Sreedharan, and I. Ray, "From Cyber Attacks to System Recovery: A Resiliency-Centered View of Cyber-Physical Systems Security." in *2026 CAE Cybersecurity Community Symposium*, Pittsburgh, Pennsylvania, 2026, pp. 74. [Abstract Link](#)

Submitted Conference

1. F. G. Arellano and **R. Podder**, "From Fix Commits to Vulnerable Functions: Automated Patch Mining for Function-Level CVE Resolution," in *Proceedings of the 2026 Workshop on Software Supply Chain Offensive Research and Ecosystem Defenses (SCORED)*, 2026, Co-located with ACM CCS 2026.
2. **R. Podder**, V. Koscinski and I. Ray, "CAPE — Context-Aware Prioritization Engine for Vulnerability Scoring and Management," in *Proceedings of the 49th International Conference on Software Engineering (ICSE)*, 2027.
3. S. K. Bashir, P. D. Hopkins, **R. Podder**, S. Shreedharan, I. Ray and I. Ray, "AWARE-RG: Abstraction

Aware Explanation of Resiliency Graphs for Cyber Physical Systems,” in *Proceedings of the 48th IEEE Symposium on Security and Privacy*, 2027.

4. **R. Podder**, P. D. Hopkins, S. K. Bashir, S. Shreedharan, I. Ray and I. Ray, “Safety Graph: When Safety Responses Become Attack Surfaces in Cyber-Physical Systems,” in *Proceedings of the Network and Distributed System Security (NDSS) Symposium*, 2026.

Submitted Journal

1. S. K. Bashir, **R. Podder**, S. Sreedharan, I. Ray, and I. Ray, “AFROT: A Framework for Modeling and Analyzing Cascading Failures in CPS Triggered by Cyber Attacks,” *IEEE Transactions on Dependable and Secure Computing*, 2026.
2. E. Rovianto, S. D. Prasetyo, C. Harsito, S. R. Joshua, **R. Podder**, A. Y. Indrarahman, and A. N. S. Permata, “Artificial Intelligence–Based Energy Management in Hybrid Biomass–Storage–EV Microgrids: A Systematic Review and Meta-Analysis,” *Green Technologies and Sustainability*, 2026.

Patents

1. **R. Podder**, S. K. Bashir, S. Sreedharan, I. Ray, and I. Ray, “Instructable AI Agent For Explainable Cybersecurity Planning and Analysis,” U.S. Provisional Patent Application Serial No. 63/839,787, filed on July 7, 2025 [APPROVED].
2. **R. Podder**, S. K. Bashir, S. Sreedharan, I. Ray, and I. Ray, “System and Methods for Building an Instructable AI Agent for Explainable Cybersecurity Planning and Analysis,” U.S. Full Patent Application, filed on July 7, 2026 [SUBMITTED].

Research Funding

U.S. Office of Naval Research (ONR)

Explainable AI for Prioritizing and Deploying Defenses for Cyber-Physical System Resiliency
Role: PhD Researcher (PIs: Indrajit Ray, Indrakshi Ray, Sarath Shreedharan)

Contract No. N000142612041 (***Helped on writing the Grant**)

Role: Assisted with the ONR proposal draft and foundational technology, and provided preliminary data.

IUCRC CCA - U.S. National Science Foundation (NSF)

Improving Cyber Security Robustness, Resiliency and Management From Devices to Enterprises

Role: PhD Researcher (PIs: Indrajit Ray, Indrakshi Ray)

Grant No. CNS 1822118 and CNS 2226232

U.S. Department of Energy (DoE)

Cyber Risk Research

Role: PhD Researcher (PI: Indrakshi Ray)

Contract No. DE-NE0008986

National Institute of Standards and Technology (NIST)

Role: PhD Researcher (PIs: Indrajit Ray, Indrakshi Ray)

Award No. 60NANB23D152.

State of Colorado

Role: PhD Researcher (PI: Indrakshi Ray)

Grant #SB 18-086.

U.S. National Science Foundation (NSF)

Role: PhD Researcher (PIs: Indrajit Ray, Indrakshi Ray)

Award No. DMS 2123761

American Megatrends International LLC

Hardware Root of Trust (HRoT) for Firmware Security

Role: PhD Researcher (PIs: Indrajit Ray)

Awards/Honors Received

2026	"Computer Science Graduate Fellowship" Award College of Natural Sciences, Colorado State University Prize: \$ 6250
2026	"Certificate of Academic Excellence" Award Colorado State University
2025	"Student Travel Grants" Award IEEE CIC/TPS/CogMI 2025 Conference Prize: \$ 700
2025	"Robert B. France Fellowship in Computer Science" Award Department of Computer Science Colorado State University Prize: \$ 2400
2025	"GSC Conference Travel Grant" Award Graduate Student Council Colorado State University Prize: \$ 500
2025	"Excellence in Teaching" Award Colorado State University
2024	"Best Paper" Award IEEE TPS-ISA 2024 Conference The Darcy, D.C., USA Paper: Resiliency Graphs: Modelling the Interplay between Cyber Attacks and System Failures through AI Planning
2024	"Best Paper" Award IEEE QRS 2024 Conference Churchill College, Cambridge, United Kingdom Paper: The PIT-Cerberus Framework: Preventing Device Tampering During Transit Prize: \$ 450
2024	"GSC Conference Travel Grant" Award Graduate Student Council Colorado State University Prize: \$ 500
2024	"GSC Conference Travel Grant" Award Graduate Student Council Colorado State University Prize: \$ 250
2023	"Certificate of Academic Excellence" Award Colorado State University
2018	"AICTE Post Graduate Scholarship" All India Council for Technical Education, Indian Government Prize: ₹12,500/month for 2 years.
2014	"Top Class Undergraduate Scholarship" Ministry of Human Resource Development (MHRD), Indian Government Prize: ₹75,000/Year for 4 years.
2013	"Dr. B R Ambedkar" Award West Bengal State Government, India Prize: ₹100,000.

Professional Appointments

Jan. 2026 – present Colorado (USA)	Graduate Research Assistant Colorado State University Department of Computer Science
Feb. 2026 – Jun. 2026 Colorado (USA)	Graduate Mentor Office for Undergraduate Research and Artistry Colorado State University, Fort Collins, CO, USA
May 2024 – May 2026 Gaithersburg (USA)	Foreign Research Scientist National Institute of Standards and Technology (NIST) Department of Computer Science
Aug 2025 – Dec. 2025 Colorado (USA)	Graduate Teaching Assistant Colorado State University Department of Computer Science
May 2022 – Aug. 2025 Colorado (USA)	Graduate Research Assistant Colorado State University Department of Computer Science
Jun. 2021 – Apr. 2022 Bhubaneswar (India)	Systems Engineer Infosys Ltd.
Nov. 2020 – May 2021 Kolkata (India)	Programmer Analyst Cognizant Technology Solutions India Private Ltd.
May 2016 – July 2016 Bokaro (India)	Summer Intern Chandrapura Thermal Power Station, DVC.

Academic Experience

Research Experience

Colorado State University
Graduate Research Assistant

Fort Collins, CO, USA
May 2022 – Present

- **CPS security and resiliency analysis via AI planning:**
 - *SPEAR* / *i-EXAM* – attack-connectivity graph modeling and hardening analysis; developed *i-EXAM*, an AI-planning and LLM-powered tool enabling system administrators to build network security profiles and run what-if hardening analyses.
 - *Resiliency Graph* (RG) / *Safety Graph* (SG) – unified frameworks modeling how cyber attacks propagate into system failures across IT and OT domains in cyber-physical systems.
 - *SERA* – an AI-driven, re-programmable simulation environment for explainable resiliency analysis, supporting both offensive/defensive security research and a teaching module for cybersecurity education.
- **CAPE (Context-Aware CVE Prioritization Engine)** – standalone publication effort. Scores CVEs reported against a project's SBOM using reachability and patch-presence evidence to suppress scanner false positives, then re-ranks surviving vulnerabilities with a 4-dimension, AHP-weighted priority score.
- **OSCAR** – cross-level risk propagation framework linking code-level risk metrics to ecosystem-level dependency exposure via a unified risk formula, to surface false-positive CVE alerts and structurally critical micro-dependencies otherwise missed by dependency-count-based tools.
- **Firmware security infrastructure** – designed and open-sourced a secure firmware remote update framework (*S-RFUP*), a protection-in-transit protocol (*PIT*), and a CDDL mapping schema for firmware manifests (*CoDICE*), built on Microsoft Project Cerberus and Google Open-DICE.

National Institute of Standards and Technology (NIST)**Gaithersburg, MD, USA***Foreign Research Scientist**May 2024 – May 2026*

- Worked with [Irena Bojanova](#) on the [Bugs Framework \(BF\)](#), applying its formal language to causally classify security bugs and formalize CVE/CWE specifications.

Teaching Experience

Teaching and lab-design experience in computer networks and cybersecurity at the undergraduate and graduate level, alongside graduate coursework spanning AI, computer architecture, and cyber-physical systems.

Colorado State University**Fort Collins, CO, USA***Graduate Teaching Assistant**Aug 2025 – Dec 2025*

- Teaching assistant for CS457 (Computer Networks and the Internet); assisted with course design and led recitation sessions.
- Delivered course lectures independently, with faculty authorization, in the instructor's absence on 4 occasions.
- Designed exam questions and grading for CS457, contributing directly to course assessment.
- Led a weekly Guidance, Study and Tutorial (GST) session during office hours: revised lecture material and worked through problem sets with students.
- Designed labs for CS557 (Advanced Networking), including penetration-testing exercises, binary reverse-engineering labs, and other hands-on offensive-security exercises.
- Supported student research and project development in CS556 (Computer Security).
- Guided graduated student as external observer on "How to handle peer-review process and analyses research paper?" for [Usable Formal Methods for Security/Privacy](#), CS 580B4 by McKenna McCall (Instructor).
- Awarded *Excellence in Teaching* by CSU for applying active-learning techniques grounded in Bloom's Taxonomy to recitation and lab design (see Awards).

Office for Undergraduate Research and Artistry (OURA), CSU**Fort Collins, CO, USA***Graduate Mentor**Feb 2026 – Jun 2026*

- Guided undergraduate mentees through research projects, provided academic and research advising, and supported development of critical-thinking and research skills.

Cybersecurity Camp Summer Program**Fort Collins, CO, USA***Instructor / Camp Designer**2023 – 2025*

- Designed lectures, hands-on activities, and classroom exercises for week-long cybersecurity day camps serving 35–50+ high school students annually across three years.
- Gained direct experience managing classroom-scale instruction and adapting technical material for varied skill levels.

Pedagogical training: Completed CSU Institute for Learning and Teaching certifications in Best Practices in Teaching, Critical Thinking Development, Inclusive Pedagogy, and Accessible Electronic Content – applied directly to course, lab, and mentoring design above (see Scientific Trainings for full list).

Industrial Experience**AMI US Holdings Inc.****Fort Collins, Colorado***Summer Intern**May 2023 – Aug 2023*

Directed research to design 100+ firmware update APIs (lib. "S-RFUP") with privileged access controls and rollback protection, 20+ (lib. "PIT") secure boot APIs enforcing identity-based device authentication and "Co-DICE" framework for CDDL mappings of firmware manifest in BMC.

Infosys Ltd.*Systems Engineer*

Transformed data between formats (30+ mapping tree) using IBM WebSphere, led team to optimize data handling efficiencies. Delivered more than 100 client requests of customised maps for various data formats.

Bhubaneswar, India*Jun 2021 – Apr 2022***Cognizant Technology Solutions India Private Ltd.***Programmer Analyst*

Specialized in Selenium for automated test planning and quality assurance in software development across 10+ projects.

Kolkata, India*Nov 2020 – May 2021***Mentoring Experience**

Wadia Ganim	Engineer Illinois ARCS Singapore (*1 Research Paper)
Sachin Kurup	CSU Intern BTech Computer Science Amrita Vishwa Vidyapeetham
Matthew Leman	Undergraduate Computer Science Department CSU
Saswat Subhankar	Undergraduate Intern Computer Science Department CSU
Enock Apedjinou	OURA Mentee Computer Science Department CSU
Jason Simental	Undergraduate Researcher Computer Science Department CSU (*1 Research Paper)
Tyler Rios	Graduate Student Computer Science Department Denver University (*1 Research Paper)
Jack Sovereign	Software Engineer Ductus (*1 Research Paper)

Presentations

Conference Presentations

- Title:** *i-EXAM: Instructable and Explainable Attack Connectivity Graph Modeler*. **Location:** The 36th International Conference on Automated Planning and Scheduling (ICAPS 2026), Dublin, Ireland, 2026.
- Title:** *CoDICE: Roll the DICE for Firmware Attestation*. **Location:** The 2025 IEEE 7th International Conference on Trust, Privacy and Security in Intelligent Systems, and Applications (TPS-ISA), Pittsburgh, PA, USA, 2025.
- Title:** *Resiliency Graphs: Modelling the Interplay between Cyber Attacks and System Failures through AI Planning*. **Location:** The 2024 IEEE 6th International Conference on Trust, Privacy and Security in Intelligent Systems, and Applications (TPS-ISA), The Darcy, Washington, DC, USA, 2024.
- Title:** *Impact of White-Box Adversarial Attacks on Convolutional Neural Networks*. **Location:** The 2024 International Conference on Emerging Trends in Networks and Computer Communications (ETNCC), Windhoek, Namibia, 2024.
- Title:** *The PIT-Cerberus Framework: Preventing Device Tampering During Transit*. **Location:** The 2024 IEEE 24th International Conference on Software Quality, Reliability and Security (QRS), The Churchill College, Cambridge, United Kingdom, 2024.
- Title:** *Hybrid Encryption Algorithm for the Data Security of ESP32 based IoT-enabled Robots*. **Location:** The 2021 Innovations in Energy Management and Renewable Resources, Kolkata, India, 2021.

Poster Presentations

- Title:** *Correctness and Security Analysis of the Protection In Transit (PIT) Protocol*. **Location:** NSF IUCRC Center for AI-ML Driven Research in Infrastructure Trust Assurance (AMRITA) Meeting,

University of Wyoming (UW), Laramie, WY, 2025.

2. **Title:** *Preventing Malicious Modifications to Firmware using Hardware Root of Trust (HROt)*. **Location:** NSF IUCRC Center for AI-ML Driven Research in Infrastructure Trust Assurance (AMRITA) Meeting, University of Wyoming (UW), Laramie, WY, 2025.
3. **Title:** *S-RFUP: Secure Remote Firmware Update Protocol*. **Location:** Graduate Student Showcase, Graduate School, Colorado State University, Fort Collins, CO, 2025.
4. **Title:** *Explainable AI for Cybersecurity and Resiliency of Nuclear Power Plant*. **Location:** The 4th Big Data for Nuclear Power Plants Workshop, Columbus, Ohio, 2024.
5. **Title:** *Correctness and Security Analysis of Protection in Transit (PIT) Protocol*. **Location:** Graduate Student Showcase, Graduate School, Colorado State University, Fort Collins, CO, 2024.
6. **Title:** *How "PIT" Libraries Work?*. **Location:** NSF IUCRC Center for Cybersecurity Analytics and Automation (CCAA) IAB Meeting 2024, George Mason University, Fairfax, VA, 2024.
7. **Title:** *Preventing Device Tampering During Transit using the Cerberus PIT Library and BIOS/BMC Boot Process Lockdown*. **Location:** NSF IUCRC Center for Cybersecurity Analytics and Automation (CCAA) IAB Meeting 2023, George Mason University, Fairfax, VA, 2023.
8. **Title:** *Preventing Firmware Tampering during Transit*. **Location:** NSF IUCRC Center for Cybersecurity Analytics and Automation (CCAA) IAB Meeting 2023, Colorado State University, Fort Collins, CO, 2023.
9. **Title:** *What is Project Cerberus?*. **Location:** Graduate Student Showcase, Graduate School, Colorado State University, Fort Collins, CO, 2023.
10. **Title:** *Security Concerns for TPM 2.0*. **Location:** CS793 Research Seminar Presentation, Computer Science Department, Colorado State University, Fort Collins, CO, 2023.
11. **Title:** *Implementing Protection in Transit*. **Location:** NSF IUCRC Center for Cybersecurity Analytics and Automation (CCAA) IAB Meeting, University of North Carolina at Charlotte (UNCC), Charlotte, NC, 2022.

Invited Talks

July 2026	CAE Community of Practice Cyber Research. <i>i-EXAM. A running case study.</i>
March 2026	Universitas Sam Ratulangi, Manado, Indonesia. <i>From Classical Systems to Intelligent Secure and Data-Centric Computing.</i>
October 2025	Northern Colorado ISSA, Lory Centre CSU, Fort Collins, CO, USA. <i>AI-Powered Cyber Security & Cyber Resiliency.</i>
July 2024	TMI Summer Talks, Fort Collins, CO, USA. <i>The PIT-Cerberus Framework: Preventing Device Tampering During Transit.</i>
October 2023	NSF IUCRC Center for CCAA Colorado State University, Fort Collins, CO, USA <i>Remote Firmware Updates: Preventing Firmware Tampering.</i>
April 2023	NSF IUCRC Center for CCAA George Mason University, Fairfax, VA, USA <i>Protection in Transit – What do we solve?.</i>
October 2022	NSF IUCRC Center for CCAA University of North Carolina at Charlotte (UNCC), Charlotte, USA <i>Protection in Transit: Enabling Tripartite Trust using a Mesh of Trusted Agents.</i>

Reviewer Services

Ad Hoc Reviewer – Journals

1. IEEE Transactions on Big Data (IEEE TBD), 2026 [[1 Paper](#)].
2. Journal of Electronic Testing Theory and Applications (JETTA), 2025 [[1 Paper](#)].
3. Journal of Nonlinear, Complex and Data Science (JNCDS), 2024 [[1 Paper](#)].

Ad Hoc Reviewer – Conferences

1. The 49th International Conference on Software Engineering (ICSE27) Dublin, Ireland, April 25-May 01, 2027 [[4 Papers](#)].
2. The 3rd International Conference on Electrical and Computer Engineering Researches (ICECER'26), Istanbul, Türkiye, December 03-05, 2026 [[1 Paper](#)].
3. The 6th International Conference on Electrical, Computer, Communications and Mechatronics Engineering (ICECCME'26) , Bali, Indonesia, October 15-17, 2026 [[1 Paper](#)].
4. The 31th European Symposium on Research in Computer Security (ESORICS'26), Rome, Italy, September 14-16, 2026. [[4 Papers](#)].
5. The 31st ACM Symposium on Access Control Models and Technologies (ACM SACMAT'26), Waterloo, Canada, July 8 - 10, 2026 [[3 Papers](#)].
6. The 6th International Conference on Electrical, Computer and Energy Technologies (ICECET'26), Rome, Italy, July 6-9, 2026 [[2 Papers](#)].
7. The 16th ACM Conference on Data and Application Security and Privacy (CODASPY'26), Frankfurt am Main, Germany June 23 – 25, 2026 [[1 Paper](#)].
8. The 3rd International Conference on Artificial Intelligence, Computer, Data Sciences and Applications (ACDSA'26), Boracay Island, Philippines, February 05-07, 2026 [[2 Papers](#)].
9. Workshop on Advances in Systems and Computation at the Edge and HPC Networks (ASCENT'25), ICDCN'26, Nara, Japan, January 06-09, 2026 [[2 Papers](#)].
10. The 2025 IEEE 7th International Conference on Trust, Privacy and Security in Intelligent Systems, and Applications (TPS-ISA), Pittsburgh, USA, November 11-14, 2025 [[1 Paper](#)].
11. The 2nd International Conference on Electrical and Computer Engineering Researches (ICECER'25), Antananarivo 101, Madagascar, December 06-08, 2025 [[2 Papers](#)].
12. The 2025 International Conference on Emerging Trends in Networks and Computer Communications (ETNCC'25), Windhoek, Namibia, August 05-07, 2025 [[1 Paper](#)].
13. The International Conference on Artificial Intelligence, Computer, Data Sciences and Applications (ACDSA'25), Antalya, Türkiye, August 7-9, 2025 [[2 Papers](#)].
14. The 5th International Conference on Electrical, Computer, Communications and Mechatronics Engineering (ICECCME'25) , Zanzibar, Tanzania, October 16-19, 2025 [[1 Paper](#)].
15. The 30th European Symposium on Research in Computer Security (ESORICS'25), Toulouse, France, September 22-26, 2025. [[3 Papers](#)].
16. The 29th European Symposium on Research in Computer Security (ESORICS'24), Bydgoszcz, Poland, September 16-20, 2024. [[1 Paper](#)].
17. The 14th ACM Conference on Data and Application Security and Privacy (CODASPY'24), Porto, Portugal June 19–21, 2024. [[1 Paper](#)].
18. The 28th European Symposium on Research in Computer Security (ESORICS'23), The Hague, The Netherlands, September 25-29, 2023. [[1 Paper](#)].

19. The 5th International Conference on Information Science and Systems (ICISS'22), Beijing, China, August 26-28, 2022 [[1 Paper](#)].
20. The 36th Annual IFIP WG 11.3 Conference on Data and Applications Security and Privacy (DB-Sec'22), Rutgers University, Newark, NJ, USA, July 18-20, 2022 [[1 Paper](#)].

Public Engagement

Apr. 2027 (upcoming)	Serving as Shadow PC in 49th International Conference on Software Engineering (ICSE 2027) , Apr. 25- May 1, 2027 in Dublin, Ireland.
Jan. 2027 (upcoming)	Serving as a Technical Program Committee (TPC) Member for the 2nd ASCENT Workshop (Advances in Systems and Computation at the Edge and HPC Networks), January 04-07, which was held in conjunction with the ICDCN Conference, January 04-07, 2027.
Mar. 2027 (upcoming)	Serving as a Technical Program Committee (TPC) Member for the PerRobotics 2027: Pervasive Robotics – Sensing, Intelligence, and Coordination for Human-Centered Smart Environments , a workshop co-located with IEEE PerCom 2027 in Goa, India.
Mar. 2027 (upcoming)	Serving as Registration Chair in 30th Annual Software Technology Conference (STC 2027) , May 4-6, 2027.
Jul. 2026	Participated in Human-AI ICS Cybersecurity Challenge Research Study from July-August 2026, conducted by Nemesys Insights, LLC .
Jul. 2026	Served as Artifact Evaluation Program Committee Member in The 31st ACM Symposium on Access Control Models and Technologies (ACM SACMAT 2026), Waterloo, Canada, July 8 - 10, 2026.
Jan. 2026	Served as a Technical Program Committee (TPC) Member for the ASCENT Workshop (Advances in Systems and Computation at the Edge and HPC Networks), January 06-09, which was held in conjunction with the ICDCN Conference, January 06-09, 2026.
Nov. 2025	Served as Student Volunteer in IEEE TPS 2025 , Nov. 2025.
Mar. 2025	Served as Review Committee Member in American Journal of Computer Science and Technology , Mar. 2025.
Jul. 2025	2025 Cybersecurity Camp Summer Program , July 2025 Hosted a one-week (5-day) CyberSecurity Day Camp at CSU Fort Collins and another one-week (5-day) Camp at CSU SPUR Campus for 50+ high school students.
Jul. 2024	2024 Cybersecurity Camp Summer Program , July 2024 Organized a one-week (5-day) CyberSecurity Day Camp at Colorado State University, Fort Collins, Colorado for 45+ high school students.
Jul. 2023	2023 Cybersecurity Camp Summer Program , July 2023 Organized a one-week (5-day) CyberSecurity Day Camp at Colorado State University, Fort Collins, Colorado for 35+ high school students.

Professional Affiliations

NCAE-C PhD Student Club

CAE Community of Practice Cyber Research, since May 2026

ACM – Association for Computing Machinery

Membership ID 8520334, since July 2025

IEEE – The Institute of Electrical and Electronics Engineers

IEEE Student Member, ID 100267751, since May 2024

Northern Colorado Information Systems Security Association (ISSA)

NoCo ISSA Student Member

Institute for Systems and Technologies of Information, Control, and Communication (INSTICC)– *Affiliate Member***Scientific Trainings**

May 2026 – July 2026
(Online)**Best Practices in Teaching at CSU**

TILT, Colorado State University

- 4-week Course: Best Practices in Teaching
- 4-week Course: Critical Thinking
- 4-week Course: Inclusive Pedagogy
- 4-week Course: Accessible and Inclusive Electronic Content
- 4-week Course: Inclusive Pedagogy 2

May 2026
(Online)**Graduate Student Mentor Training**The Institute for Learning and Teaching
Colorado State UniversityFeb. 2026 – July 2026
(Online)**Early Career Grants Program**

CSU WRITES, Colorado State University

- Webinar: Grant Program Information Session
- Webinar: RAO Grant Writing Overview – Early Career
- Webinar: Grants & GenAI - Strategies and Guidelines
- Webinar: Structuring Your Project Narrative with RAO
- Webinar: NSF Career Proposal Strategies

Jan. 2026
(Online)**Graduate Teaching Assistant Training**The Institute for Learning and Teaching
Colorado State UniversityOct. 2025
(In Person)**Graduate Student Mentoring Training**The Graduate School
Colorado State UniversityOct. 2025
(Online)**Excellence in Teaching**The Language, Culture, and Resources program for Excellence in Teaching
Colorado State UniversityJul. 2025
(Online)**Social / Humanistic / Behavioral Research**CITI Program
Colorado State UniversityAug. 2023 – Nov. 2023
(In Person)**Ethical Conduct of Research**The Graduate School
Colorado State University**Skills**

Languages

Native: Bengali
Other languages: English, HindiProgramming &
DevelopmentProficient: C/C++, PDDL, Python. Familiar: JavaScript, SQL, Java, Git,
Verilog HDL, $\text{\LaTeX}$ Libraries and ML
AlgorithmsTensorFlow, PyTorch, NumPy, Pandas, Matplotlib, Scikit-Learn, Seaborn,
ART, cleverhans; LLM, CtmNN, Decision Trees, Transformers

Databases & Operating Systems	PostgreSQL, MySQL, MongoDB; Kali, Linux, Mac OS, Windows, Hypervisors, QEMU, Virtual Box, VMware, Docker
Tools & Technologies	Splunk, ELK, CAN, STRIDE, GNS3, TLA+, Wazuh, Caldera, OPNsense, pfSense, CPN, Wireshark, Google Colab, Heroku, Azure, Jupyter Notebook, UPPAAL, Syft, x86, ARM, MITRE ATT&CK, Suricata, Procmon, Grype, OpenVAS, Tenable, Active Directory, LLVM, NIST 800-61, ISO 27035, REMnux, Burp Suite
Open Source Projects	HexStrike AI, Project Cerberus, OpenBMC-libpldm, VAL, Forbid Iterator, Fast Downward, Open-DICE

References

Prof. Indrajit Ray

Professor and Associate Chair
Department of Computer Science
Colorado State University
Fort Collins, Colorado, 80523, USA
Email: indrajit.ray@colostate.edu
Phone: +1 (970) 420-8003

Prof. Indrakshi Ray

Director, Colorado Center for Cyber Security
Department of Computer Science
Colorado State University
Fort Collins, Colorado, 80523, USA
Email: indrakshi.ray@colostate.edu
Phone: +1 (970) 491-7986

Dr. Sarath Sreedharan

Assistant Professor
Department of Computer Science
Colorado State University
Fort Collins, Colorado, 80523, USA
Email: sarath.sreedharan@colostate.edu
Phone: +1 (970) 491-7008