

Debopriya Roy Dipta

Department of Electrical and Computer Engineering
The University of Akron, Akron, OH

Phone: (+1) 515-203-9927
Email: ddipta@uakron.edu
Webpage | LinkedIn | Google Scholar

RESEARCH INTERESTS

My research spans systems security and computer architecture, with a focus on microarchitectural side-channel attacks and defenses. I study how hardware and operating-system features such as dynamic frequency scaling, energy reporting, and shared caches leak information across isolation boundaries, from browsers and mobile devices to containers, sandboxes, and Trusted Execution Environments (TEEs) in the cloud. I also develop learning-based techniques to detect and mitigate these attacks, evaluate the robustness of such detectors against evasion, and build LLM-driven agentic frameworks that automate the generation of microarchitectural attack proof-of-concepts.

PROFESSIONAL EXPERIENCE

- **Assistant Professor (Tenure-Track), Department of Electrical and Computer Engineering, The University of Akron**, Aug 2026 - Present.
- **Research Assistant, Microarchitecture and Artificial Intelligence Security Laboratory (MAIS), Iowa State University**, Aug 2021 - Nov 2024, Aug 2025 - Aug 2026.
Investigated side-channel and speculative execution vulnerabilities, including new leakage pathways in containers, sandboxes, TEEs, and serverless cloud systems; designed deep learning-based detection and mitigation techniques; and developed uGen, an agentic framework for generating microarchitectural attack proof-of-concepts with LLMs.
- **Research Intern, Telefónica Innovación Digital, Barcelona, Spain**, Nov 2024 - Apr 2025.
Analyzed co-location methods in cloud environments and evaluated the feasibility of microarchitectural side-channel attacks in serverless platforms, particularly Cloudflare's infrastructure.
- **Research Administration Intern, Centre for Multiphase Flow Research and Education (CoM-FRE) and Iowa Water Center (IWC), Iowa State University**, May - Aug. 2025.

EDUCATION

Iowa State University	Ames, IA
Ph. D. in Computer Engineering	August 2026
Dissertation: <i>From Manual Exploration to Automated Analysis of Microarchitectural Threats</i>	
Advisor: Dr. Berk Gulmezoglu	
Iowa State University	Ames, IA
M. Eng. in Computer Engineering	August 2024
Khulna University of Engineering and Technology	Khulna, Bangladesh
B. Sc. in Electrical and Electronic Engineering	April 2018

PUBLICATIONS

Preprints and Pending Papers

1. **D. R. Dipta**, T. Tiemann, E. Marin, T. Eisenbarth and B. Gulmezoglu, "uGen: An Agentic Framework for Generating Microarchitectural Attack PoCs," under review, *arXiv preprint arXiv:2605.15503*, 2026.
2. **D. R. Dipta**, E. Marin, B. Gulmezoglu and T. Eisenbarth, "Exploiting and Mitigating Information Leakage at the Container-Kernel Interface," in preparation.
3. **D. R. Dipta**, K. Christofferson, S. Son and B. Gulmezoglu, "DimShield: Exploring Intrinsic Dimension Estimation for Enhanced Machine Learning Security," in preparation.

Conference Papers

4. **D. R. Dipta**, T. Tiemann, B. Gulmezoglu, E. Marin and T. Eisenbarth, "Dynamic Frequency-Based Fingerprinting Attacks against Modern Sandbox Environments," *2024 IEEE 9th European Symposium on Security and Privacy (EuroS&P)*, pp. 327-344, Vienna, Austria, 2024.
5. S. Son, **D. R. Dipta** and B. Gulmezoglu, "DefWeb: Defending User Privacy against Cache-based Website Fingerprinting Attacks with Intelligent Noise Injection," *Proceedings of the 39th Annual Computer Security Applications Conference (ACSAC '23)*, pp. 379-393, 2023.
6. **D. R. Dipta** and B. Gulmezoglu, "DF-SCA: Dynamic Frequency Side Channel Attacks are Practical," *Proceedings of the 38th Annual Computer Security Applications Conference (ACSAC '22)*, pp. 841-853, 2022.

Journal Articles

7. **D. R. Dipta**, J. Tan and B. Gulmezoglu, "Systematical Evasion From Learning-Based Microarchitectural Attack Detection Tools," *IEEE Journal on Emerging and Selected Topics in Circuits and Systems (IEEE JETCAS)*, vol. 14, no. 4, pp. 823-833, Dec. 2024.
8. **D. R. Dipta** and B. Gulmezoglu, "MAD-EN: Microarchitectural Attack Detection Through System-Wide Energy Consumption," *IEEE Transactions on Information Forensics and Security (IEEE TIFS)*, vol. 18, pp. 3006-3017, 2023.

Earlier Publications (Energy Systems, Machine Learning Applications, Hardware)

9. S. Tabassum, T. Rahman, A. U. Islam, S. Rahman, **D. R. Dipta**, S. Roy, N. Mohammad, N. Nawar and E. Hossain, "Solar Energy in the United States: Development, Challenges and Future Prospects," *Energies*, 14(23), Article 8142, 2021.
10. E. Hossain, S. Roy, N. Mohammad, N. Nawar and **D. R. Dipta**, "Metrics and Enhancement Strategies for Grid Resilience and Reliability during Natural Disasters," *Applied Energy*, vol. 290, 2021.
11. A. A. Mamun, M. Sohel, N. Mohammad, M. S. Haque Sunny, **D. R. Dipta** and E. Hossain, "A Comprehensive Review of the Load Forecasting Techniques Using Single and Hybrid Predictive Models," *IEEE Access*, vol. 8, pp. 134911-134939, 2020.
12. M. S. Rahman, M. S. Hossain, E. H. Rahat, **D. R. Dipta**, H. M. R. Faruque and F. K. Fattah, "Efficient Hardware Implementation of 256-bit ECC Processor Over Prime Field," *2019 International Conference on Electrical, Computer and Communication Engineering (ECCE)*, Bangladesh, 2019.
13. M. S. Haque Sunny, **D. R. Dipta**, S. Hossain, H. M. Resalat Faruque and E. Hossain, "Design of a Convolutional Neural Network Based Smart Waste Disposal System," *2019 1st International Conference on Advances in Science, Engineering and Robotics Technology (ICASERT)*, Dhaka, Bangladesh, 2019.
14. F. I. Bappy, M. Jahirul Islam, A. K. Podder, **D. R. Dipta**, H. M. Resalat Faruque and E. Hossain, "Comparison of Different Hybrid Renewable Energy Systems With Optimized PV Configuration to Realize the Effects of Multiple Schemes," *2019 1st International Conference on Advances in Science, Engineering and Robotics Technology (ICASERT)*, Dhaka, Bangladesh, 2019.
15. M. M. Rahman, **D. R. Dipta** and M. M. Hasan, "Dynamic Time Warping Assisted SVM Classifier for Bangla Speech Recognition," *2018 International Conference on Computer, Communication, Chemical, Material and Electronic Engineering (IC4ME2)*, Rajshahi, Bangladesh, 2018.

TEACHING/MENTORING EXPERIENCE

-
- **Instructor, The University of Akron**, Fall 2026 - Present.
 - ELEN 230, Circuits Laboratory (Fall 2026)
 - ELEN 441/541, Digital Communication (Fall 2026, co-taught)
 - ELEN 401, Senior Design Project (Fall 2026)
 - CPEN 427/527, Computer Networks (Spring 2027, upcoming)
 - **Teaching Assistant, Iowa State University**, Spring & Fall 2024.
CPR E 538, Reverse Engineering and Security Testing. Prepared and conducted lab sessions on software reverse engineering, malware analysis, and microarchitectural security concepts.

- **Undergraduate Research Mentor, MAIS Lab, Iowa State University**, 2023 – 2025.
Mentored three undergraduate researchers in machine learning and hardware security, leading to the IEEE JETCAS paper and the DimShield project.
- **Research Mentor, Academic Program for EXcellence for Engineers (APEX^E), Iowa State University**, Summer 2023.
Mentored an undergraduate project, “Cache Occupancy-based Side-Channel Attack to Fingerprint Docker Images,” culminating in a research poster.
- **Senior Design Project Mentor, Iowa State University**, Fall 2022 – Spring 2023.
CPR E 491/492. Supervised a six-student team that built a framework combining Intel RAPL-based energy measurements with adversarial code generation to evaluate the robustness of microarchitectural attack detection tools.

TALKS & POSTER PRESENTATIONS

Talks

1. *(Invited)* “Exploiting Dynamic Frequency: Side-Channel Attacks and Evasion in Modern Systems,” University of Lübeck, Germany, Apr. 2025.
2. *(Invited)* “Dynamic Frequency-Based Side-Channel Attacks on Modern Computing Environments,” CAE-R Symposium, St. Louis, Oct. 2024.
3. “Dynamic Frequency-Based Fingerprinting Attacks against Modern Sandbox Environments,” IEEE EuroS&P, Vienna, Austria, July 2024.
4. “DF-SCA: Dynamic Frequency Side Channel Attacks are Practical,” ACSAC ’22, Austin, TX, Dec. 2022.
5. *(Invited)* “DF-SCA: Dynamic Frequency Side Channel Attacks are Practical,” NVIDIA, July 2022.

Poster Presentations

6. *(Invited)* “DF-SCA: Dynamic Frequency Side Channel Attacks are Practical,” Youth Cyber Summit, Iowa Cyber Hub, 2025.
7. *(Invited)* “Dynamic Frequency-Based Fingerprinting Attacks against Modern Sandbox Environments,” CAE-R Symposium, St. Louis, 2024.
8. *(Invited)* “DF-SCA: Dynamic Frequency Side Channel Attacks are Practical,” CEAB, Iowa Cyber Hub, 2023.

ACADEMIC HONORS

- Miller Completion Award, Iowa State University, Summer 2026. Awarded for completing doctoral studies with outstanding research accomplishments.
- Research Excellence Award (REX), Graduate College, Iowa State University, May 2026. Recognizes graduate students who have demonstrated outstanding accomplishments in research and scholarly achievement.
- Takano Fellowship Graduate Research Fellowship (for 1 academic year, ≈\$60K), Iowa State University, 2025–2026.
- Glenn W. and Cordelia R. Sellers Graduate Research Endowment (\$6K), Iowa State University, 2023–2024.
- ACSAC Student Conferencship, 2022.
- University Merit Scholarship, Khulna University of Engineering and Technology, 2013–2018.

PROFESSIONAL SERVICE & DEVELOPMENT

- Reviewer (Journals) - *IEEE Transactions on Information Forensics and Security* (2024, 2025), *IEEE Transactions on Dependable and Secure Computing* (2025), *IEEE Open Journal of the Computer Society* (2025), *IEEE Access* (2020-2021).
- Reviewer (Conferences) - *ESORICS* (2023, 2024), *NDSS* (2025).
- Participant, 2026 NSF SaTC Aspiring PIs Workshop, Washington, DC, Oct. 2026.
- Presenter, Youth Cyber Summit, Iowa Cyber Hub (2024, 2025) - Cybersecurity awareness demonstrations for high school students.
- Vice-President, IEEE Student Branch, KUET, Bangladesh, 2016-2018.