Debopriya Roy Dipta

2025 Long Rd, Unit C
Ames, IA-50010

Phone: (+1) 515-203-9927
Email: roydipta@iastate.edu
LinkedIn | Google Scholar

EDUCATION

Iowa State University — Ames, IA
Ph. D. in Computer Engineering — *2021-Present*
Expected Graduation June 2026

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*

RESEARCH INTERESTS

My research interests span the areas of side-channel attacks, system security, computer architecture, and artificial intelligence. My research explores how artificial intelligence can both expose and defend against side-channel attacks, working at the intersection of computer architecture and cybersecurity to make computing systems more secure without sacrificing performance.

WORK EXPERIENCE

- **Research Assistant, Microarchitecture and Artificial Intelligence Security Laboratory (MAIS), Iowa State University**, Aug 2021 - Nov 2024, Aug 2025 - Present.

  As a Research Assistant at MAIS, I primarily investigate microarchitectural and software-level attack vectors, focusing on side-channel and speculative execution vulnerabilities. My work extends to exploring new leakage pathways in Trusted Execution Environments (TEEs) and sandboxed serverless cloud systems, exposing how isolation mechanisms can be bypassed. Alongside attack development, I also contribute to designing deep learning–based detection and mitigation techniques. Currently, I am developing an LLM-assisted multi-agent framework that autonomously generates, tests, and improves both attack and defense strategies, advancing automated security evaluation across architectures.

- **Research Administration Intern, Centre for Multiphase Flow Research and Education (CoMFRE) and Iowa Water Center (IWC), Iowa State University**, May - Aug. 2025.

  During my internship, I supported both pre-award and post-award research administration by contributing to grant preparation, budget planning, and faculty outreach. I also assisted with website management and digital accessibility updates to ensure compliance with accessibility standards across research centers. This role strengthened my understanding of academic project management and enhanced my ability to translate complex research outcomes into accessible content for funding agencies, collaborators, and broader audiences.

- **Research Intern, Telefónica Innovación Digital, Barcelona, Spain**, Nov 2024 - Apr 2025.

  At Telefónica's Digital Innovation Lab, I worked on identifying and analyzing co-location methods within cloud environments to assess their susceptibility to microarchitectural side-channel attacks. My research focused on evaluating the feasibility of such attacks in serverless paradigms, particularly targeting Cloudflare's infrastructure. This experience deepened my perspective on the intersection of cloud security and hardware-level vulnerabilities while exposing me to real-world challenges faced by global telecommunication and cloud service providers.

TEACHING/MENTORING EXPERIENCE

- **Teaching Assistant, Iowa State University,** Spring & Fall 2024.
  Course: CPR E 538, Reverse Engineering and Security Testing
  Prepared and conducted lab sessions on software reverse engineering, malware analysis, and microarchitectural security concepts. Supported student learning through office hours, exam and assignment grading, and guidance on using open-source malware analysis tools.
- **Undergraduate Research Mentor, Microarchitecture and Artificial Intelligence Security Laboratory (MAIS), Iowa State University**, 2023 – 2025.
  Mentored multiple undergraduate researchers (3 students) on projects exploring the intersection of machine learning and hardware security. One of these mentorships led to the publication of the paper "Systematical Evasion From Learning-Based Microarchitectural Attack Detection Tools" in a peer-reviewed journal. Another ongoing project under my supervision focuses on DimShield, a runtime defense framework for adversarial attacks, which is currently under preparation for journal submission.
- **Research Mentor, Academic Program for EXcellence for Engineers (APEX^E), Iowa State University**, 2023 Cohort (Summer)
  Mentored Sebastian De La Torre, an undergraduate student, in the APEX^E research program on a project titled "Cache Occupancy-based Side-Channel Attack to Fingerprint Docker Images." The work culminated in a research poster presentation.
- **Senior Design Project Mentor, Iowa State University**, Fall 2022 – Spring 2023.
  Course: CPR E 491, Senior Design Project I; CPR E 492, Senior Design Project II
  Supervised a senior design team (group of six) that developed a framework to evaluate the robustness of microarchitectural attack detection tools against adversarial AI-based attacks. The team implemented an end-to-end prototype combining Intel RAPL-based energy measurements with adversarial code generation and a graphical user interface for testing. This mentorship concluded with a successful poster presentation demonstrating the working prototype and research outcomes.

PUBLICATIONS

Conference Papers

Topics: Side-channel attack, System Security, Machine Learning

1. **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.
2. S. Son, **D. R. Dipta** and B. Gulmezoglu, "DefWeb: Defending User Privacy against Cache-based Website Fingerprinting Attacks with Intelligent Noise Injection." *In Proceedings of the 39th Annual Computer Security Applications Conference (ACSAC '23).* Association for Computing Machinery, New York, NY, USA, 379–393, 2023.
3. **D. R. Dipta** and Berk Gulmezoglu, "DF-SCA: Dynamic Frequency Side Channel Attacks are Practical," In *Proceedings of the 38th Annual Computer Security Applications Conference (ACSAC '22).* Association for Computing Machinery, New York, NY, USA, 841–853, 2022.

Topics: Cryptography, Signal/Image Processing, Renewable Energy, Machine Learning

4. 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.
5. 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.
6. 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.
7. 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.

Journal Articles

Topics: Side-channel attack, System Security, Cryptography, Machine Learning

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

Topics: Renewable Energy, Optimization, Machine Learning

10. S. Tabassum, T. Rahman, A.U. Islam, S. Rahman, **D. R. Dipta**, S. Roy, N. Mohammad, N. Nawar, E. Hossain, "Solar Energy in the United States: Development, Challenges and Future Prospects. *Energies, 14(23), Article 8142*, 2021.
11. E. Hossain, S. Roy, Naeem Mohammad, N. Nawar, **D. R. Dipta**, Metrics and enhancement strategies for grid resilience and reliability during natural disasters, *Applied Energy, Volume 290*, 2021.
12. 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," in *IEEE Access, vol. 8, pp. 134911-134939*, 2020.

Pending Papers

13. "uGen: From Gaps to Exploits — A Multi-Agent, Retrieval-Augmented System for End-to-End Microarchitectural Attack Code Generation," with T. Tiemann, B. Gulmezoglu, E. Marin and T. Eisenbarth.
14. "DimShield: Exploring Intrinsic Dimension Estimation for Enhanced Machine Learning Security," with K. Christofferson, S. Seonghun, B. Gulmezoglu.
15. "Exploiting and Mitigating Information Leakage at the Container-Kernel Interface," with E. Marin, B. Gulmezoglu, and T. Eisenbarth.

TALKS & POSTER PRESENTATION

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 Fingerprinting Attacks against Modern Sandbox Environments," EURO S&P, Viena, Austria, July 2024.
3. *(Invited)* "Dynamic Frequency-Based Side-Channel Attacks on Modern Computing Environments," CAE-R Symposium in St. Louis, Oct 2024.
4. *(Invited)* "DF-SCA: Dynamic Frequency Side Channel Attacks are Practical", NVIDIA, July 2022.
5. *(Invited)* "DF-SCA: Dynamic Frequency Side Channel Attacks are Practical", ACSAC'22, Texas, Dec. 2022.

Poster Presentation

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, 2025.

ACADEMIC HONORS

- Takano Fellowship Graduate Research Fellowship (For 1 academic year, $\approx$ \$60K), Iowa State University, 2025–2026.
- Glenn W. and Cordelia R. Sellers Graduate Research Endowment ($6K), Iowa State University, 2023–2024.
- ACSAC Student Conferenceship, 2022.
- University Merit Scholarship, Khulna University of Engineering and Technology, 2013–2018.

SERVICE

- Reviewer (Journals) - *IEEE Transactions on Information Forensics and Security (2024, 2025), IEEE Transaction on Dependable and Secure Computing (2025), IEEE Open Journal of the Computer Society (2025), IEEE Access (2020-2021).*
- Reviewer (Conferences) - *ESORIC (2023, 2024), NDSS (2025)*
- Presenter, Youth Cyber Summit (2024, 2025) - Engaged high school students in a cybersecurity awareness demonstration organized by the Iowa Cyber Hub and led by Dr. Doug Jacobson, promoting early cyber education and safe computing practices.
- Vice-President of IEEE Student Branck, KUET, Bangladesh, 2016-2018.

REFERENCES

Dr. Berk Gulmezoglu
Assistant Professor
Iowa State University
Phone: +1 (515) 294-1404
bgulmez@iastate.edu

Dr. Thomas Eisenbarth
Professor
University of Lübeck, Germany
Phone: +49 (451) 3101 6600
thomas.eisenbarth@uni-luebeck.de

Dr. Eklas Hossain
Associate Professor
Boise State University
Phone: +1 (414) 248-7089
eklashossain@boisestate.edu