

# Aritra Dhar, Ph.D.

✉ aritra.dhar7@gmail.com  
☎ +41779448684  
🌐 www.aritradhar.com  
🌐 www.linkedin.com/in/aritradhar  
🎓 scholar.google.com/citations?hl=en&user=Icgn4goAAAAJ  
📍 Zurich, Switzerland

## Core Competencies

- ✦ Hands-on experience and expertise in trusted computing, AI Security, and secure agentic systems. Publications in top-tier security & system conferences. Multiple patents in system design.
- ✦ Experienced in full-stack system simulation and development: from hardware design, and development of software components to real-world deployment and realistic workload.
- ✦ Experienced in leading projects, building teams from the ground up, finding challenging research and project direction, and innovation in industry and academia.

## Experiences

- 11/2024 – .. ✦ **Principal Researcher - AI Security.** Computing System Laboratory, Huawei Zurich Research Center, Zurich, Switzerland.
- 08/2021 – 11/2024 ✦ **Senior Researcher - Hardware Security.** Computing System Laboratory, Huawei Zurich Research Center, Zurich, Switzerland.
- 12/2014 – 04/2016 ✦ **Research Engineer.** Xerox Research Center India, Bangalore, India.
- 01/2013 – 07/2013 ✦ **Research Intern.** Accenture Technology Labs, Bangalore, India.

## Education

- 2016 – 2021 ✦ **Ph.D., Computer Science, ETH Zurich, Switzerland**  
Advisor: Dr. Srdjan Čapkun, System Security Group  
Thesis title: *Building Trust in Modern Computing Platforms*
- 2012 – 2014 ✦ **Masters. Computer Science (Information Security), IIIT Delhi, India**  
Thesis title: *Clotho : Saving Programs from Malformed Strings and Incorrect String-handling*
- 2008 – 2012 ✦ **Bachelor. Computer Science, WBUT, India**  
Thesis title: *Security of Key Pre-distribution Schemes in Wireless Sensor Networks*

## Research Publications and Patents

### Conference Proceedings

- 1 **Dhar\***, A., Thorens\*, C., Lazier, L. M., & Cavigelli, L. (2025). Guardain: Protecting Emerging Generative AI Workloads on Heterogeneous NPU. In *IEEE S&P 2025*.
- 2 Lazier, L. M., **Dhar, A.**, Stambolic, V., & Cavigelli, L. (2025). AC-LoRA: (Almost) Training-Free Access Control-Aware Multi-Modal LLMs. In *NeurIPS 2025*.
- 3 **Dhar, A.**, Sridhara, S., Shinde, S., Capkun, S., & Andri, R. (2024a). Confidential Computing with Heterogeneous Devices at Cloud-Scale. In *ACSAC 2024*.
- 4 Schneider\*, M., **Dhar\***, A., Puddu, I., Kostiainen, K., & Capkun, S. (2022). Composite enclaves: Towards disaggregated trusted execution. In *CHES 2022*.
- 5 **Dhar, A.**, Puddu, I., Kostiainen, K., & Capkun, S. (2020). Proximatee: Hardened SGX attestation by proximity verification. In *ACM CODASPY 2020*.

- 6 **Dhar, A.**, Ulqinaku, E., Kostiainen, K., & Capkun, S. (2020). Protection: Root-of-trust for IO in compromised platforms. In *NDSS 2020*.
- 7 Mavroudis, V., Wüst, K., **Dhar, A.**, Kostiainen, K., & Capkun, S. (2020). Snappy: Fast on-chain payments with practical collaterals. In *NDSS 2020*.
- 8 Sommer, D. M., **Dhar, A.**, Malisa, L., Mohammadi, E., Ronzani, D., & Capkun, S. (2019). Deniable upload and download via passive participation. In *NSDI 2019*.
- 9 Allabadi, G., **Dhar, A.**, Bashir, A., & Purandare, R. (2018). METIS: resource and context-aware monitoring of finite state properties. In *Runtime verification RV 2018*.
- 10 Matetic, S., Ahmed, M., Kostiainen, K., **Dhar, A.**, Sommer, D. M., Gervais, A., ... Capkun, S. (2017). ROTE: rollback protection for trusted execution. In *USENIX security 2017*.
- 11 **Dhar, A.**, Nittala, A., & Yadav, K. (2016). Tactback: Vibrotactile braille output using smartphone and smartwatch for visually impaired. In *ACM web for all conference, W4A '16*.
- 12 **Dhar, A.**, Purandare, R., Dhawan, M., & Rangaswamy, S. (2015). CLOTHO: saving programs from malformed strings and incorrect string-handling. In *ESEC/FSE 2015*.
- 13 Saxena, A., Misra, J., & **Dhar, A.** (2014). Increasing anonymity in bitcoin. In *Financial cryptography and data security - FC 2014*.
- 14 Sarkar, P., Rai, B. K., & **Dhar, A.** (2013). Connecting, scaling and securing RS code and TD based kpds in wsns: Deterministic merging. In *ACM mobihoc '13*.

## Posters

- 1 **Dhar, A.**, Sridhara, S., Shinde, S., Capkun, S., & Andri, R. (2024b). *Confidential Computing with Heterogeneous Devices at Cloud-Scale* (DAC 2024). Retrieved from <https://61dac.conference-program.com/presentation/?id=RESEARCH461&sess=sess237>
- 2 **Dhar, A.**, Sridhara, S., Shinde, S., Capkun, S., & Andri, R. (2024c). *Principles for Enabling TEEs on Domain-Specific Accelerators* (DAC 2024). Retrieved from <https://61dac.conference-program.com/presentation/?id=RESEARCH460&sess=sess236>

## Journal Articles

- 1 Kostiainen, K., **Dhar, A.**, & Capkun, S. (2020). Dedicated security chips in the age of secure enclaves. *IEEE Security Privacy*, 18(5), 38–46.
- 2 Tulabandhula, T., Vaya, S., & **Dhar, A.** (2020). Privacy preserving targeted advertising and recommendations. *Journal of Business Analytics*.

## Preprints

- 1 **Dhar, A.**, Sridhara, S., Shinde, S., Capkun, S., & Andri, R. (2022). Empowering data centers for next generation trusted computing. arXiv. Retrieved from <https://arxiv.org/abs/2211.00306>
- 2 Sluganovic, I., Ulqinaku, E., **Dhar, A.**, Lain, D., Capkun, S., & Martinovic, I. (2020). Integriscreen: Visually supervising remote user interactions on compromised clients. Retrieved from <https://arxiv.org/abs/2011.13979>
- 3 **Dhar, A.**, Yu, D.-Y., Kostiainen, K., & Capkun, S. (2017). Integrikey: End-to-end integrity protection of user input. Retrieved from <https://eprint.iacr.org/2017/1245>

## Patents

- 1 **Dhar, A.**, Cavigelli, L., & Thornes, C. (2024). *Chipset, system and method for confidential computing*. WO (PCT) WO2025153164A1.

- 2 **Dhar, A.**, Cavigelli, L., & Thornes, C. (2023). *Method of establishing confidential artificial intelligence infrastructure and computing device for deploying artificial intelligence model*. WO (PCT) 92043453PCT01.
- 3 Srdjan, C., **Dhar, A.**, Matetic, S., Kostianen, K., & Sommer, D. (2023). *Methods and systems for detecting rollback attacks*. WIPO (PCT) Patent WO2018104326A1.
- 4 **Dhar, A.**, Vaya, S., Singh, A., Solanki, B. S., & Sharma, S. (2020). *Method and system for displaying targeted content on a digital signage board*. US Patent 10,825,057.
- 5 **Dhar, A.**, Yu, D.-Y., & Capkun, S. (2020). *Confidentiality and integrity of user input in web pages*. WIPO (PCT) Patent WO2020083503A1.
- 6 Srdjan, C., **Dhar, A.**, Kostianen, K., Wust, K., & Mavroudis, V. (2020). *A method and system for executing fast and safe transactions involving a high-latency blockchain*. WIPO (PCT) Patent WO2021048056A1.
- 7 **Dhar, A.**, & Vaya, S. (2019). *Methods and systems for broadcasting targeted advertisements to mobile device*. US Patent 10,333,909.
- 8 **Dhar, A.**, Yu, D.-Y., & Capkun, S. (2019). *Integrity of user input in web pages*. EU Patent EP3477531A1.
- 9 Singh, A., Manjunath, G., Vaya, S., Solanki, B. S., Sharma, S., & **Dhar, A.** (2019). *Method and system for receiving targeted content*. US Patent 10,311,480.
- 10 Vaya, S., **Dhar, A.**, Solanki, B. S., Singh, A., Sharma, S., Pande, N., & Manjunath, G. (2019). *Methods and systems for interaction with digital signage board*. US Patent 10,489,824.
- 11 **Dhar, A.**, & Yadav, K. (2018). *Methods and systems for providing non-auditory feedback to users*. US Patent App. 15/607,804.
- 12 Vaya, S., **Dhar, A.**, & Tulabandhula, T. (2018). *Systems and methods for privacy preserving recommendation of items*. US Patent App. 15/417,274.

## Skills

---

Coding	■ C/C++/Embedded C, Python, Java, SystemVerilog, Datalog/Prolog, R, $\text{\LaTeX}$
Tools/Frameworks	■ PyTorch, CUDA, Soot, Intel SGX, ARM TrustZone, ARM CCA
Web Dev	■ HTML, css, JavaScript, Tomcat Web Server.