Aritra Dhar, Ph.D.

www.aritradhar.com
www.linkedin.com/in/aritradhar
scholar.google.com/citations?hl=en&user=Icgn4goAAAAJ
Zurich, Switzerland

Core Competencies

- Hands-on experience in state-of-the-art security technologies and platform security. Expertise in trusted computing, AI Security, secure agentic systems, system security, operating systems, and hypervisors. 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 grounds up, finding challenging research and project direction, and innovation in industry and academia.

Experiences

11/2024 – .. **Principal Researcher - Hardware 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.
- Secure AI agents, AI model access control and safety.
- Confidential inference, training, and fine-tuning for large language models (LLMs).
- Confidential computing and trusted execution environments for heterogeneous data centers, confidential ML/AI on Neural Processing Units (NPU).
- Security protocol design and analysis for large, distributed, shared memory data centers. Hardware design for security modules for embedded systems and complex AI accelerators.
- Leading a team for trusted computing, hardware security, secure hardware design, and embedded systems.
- Coordination of security-related projects with ETH Zurich Future Computing Labs (EFCL) and other academic collaborations.

12/2014 – 04/2016 **Research Engineer.** Xerox Research Center India, Bangalore, India.
- Privacy preserving targeted advertisement and recommendation systems
- Using smartphone and smartwatches to assist and navigate the visually impaired

01/2013 – 07/2013 **Research Intern.** Accenture Technology Labs, Bangalore, India.
- Taint analysis on Java program to detect vulnerabilities like SQL injection, XSS
- Increasing anonymity in bitcoin transaction using aggregate signature scheme

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*
- Secure user interaction and trusted path with cyber-physical systems
- Trusted path with distributed TEE enclaves
- Fast on-chain payments with practical collateral.
- Anonymous communication for participation deniability

2012 – 2014 **Masters. Computer Science (Information Security), IIIT Delhi, India**
Thesis title: *Clotho : Saving Programs from Malformed Strings and Incorrect String-handling*

Education (continued)

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.**, Sridhara, S., Shinde, S., Capkun, S., & Andri, R. (n.d.). Confidential Computing with Heterogeneous Devices at Cloud-Scale. In *ACSAC 2024*.
2. **Dhar**, **A.**, Thorens, C., Lazier, L. M., & Cavigelli, L. (2025). Guardain: Protecting Emerging Generative AI Workloads on Heterogeneous NPU. In *S&P*.
3. Schneider*, M., **Dhar***, A., Puddu, I., Kostiainen, K., & Capkun, S. (2022). Composite enclaves: Towards disaggregated trusted execution. In *CHES 2022*.
4. **Dhar**, **A.**, Puddu, I., Kostiainen, K., & Capkun, S. (2020). Proximitee: Hardened SGX attestation by proximity verification. In *ACM CODASPY 2020*.
5. **Dhar**, **A.**, Ulqinaku, E., Kostiainen, K., & Capkun, S. (2020). Protection: Root-of-trust for IO in compromised platforms. In *NDSS 2020*.
6. Mavroudis, V., Wüst, K., **Dhar**, **A.**, Kostiainen, K., & Capkun, S. (2020). Snappy: Fast on-chain payments with practical collaterals. In *NDSS 2020*.
7. Sommer, D. M., **Dhar**, **A.**, Malisa, L., Mohammadi, E., Ronzani, D., & Capkun, S. (2019). Deniable upload and download via passive participation. In *NSDI 2019*.
8. Allabadi, G., **Dhar**, **A.**, Bashir, A., & Purandare, R. (2018). METIS: resource and context-aware monitoring of finite state properties. In *Runtime verification RV 2018*.
9. 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*.
10. **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*.
11. **Dhar**, **A.**, Purandare, R., Dhawan, M., & Rangaswamy, S. (2015). CLOTHO: saving programs from malformed strings and incorrect string-handling. In *ESEC/FSE 2015*.
12. Saxena, A., Misra, J., & **Dhar**, **A.** (2014). Increasing anonymity in bitcoin. In *Financial cryptography and data security - FC 2014*.
13. 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. (2024a). *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. (2024b). *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. Lazier, L. M., **Dhar**, **A.**, Stambolic, V., & Cavigelli, L. (2025). AC-LoRA: (Almost) Training-Free Access Control-Aware Multi-Modal LLMs. Retrieved from https://arxiv.org/abs/2505.11557
2. **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
3. 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
4. **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. (2023). *Method of establishing confidential artificial intelligence infrastructure and computing device for deploying artificial intelligence model*. WO (PCT) 92043453PCT01.
2. Srdjan, C., **Dhar**, **A.**, Matetic, S., Kostiainen, K., & Sommer, D. (2023). *Methods and systems for detecting rollback attacks*. WIPO (PCT) Patent WO2018104326A1.
3. **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.
4. **Dhar**, **A.**, Yu, D.-Y., & Capkun, S. (2020). *Confidentiality and integrity of user input in web pages*. WIPO (PCT) Patent WO2020083503A1.
5. Srdjan, C., **Dhar**, **A.**, Kostiainen, 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.
6. **Dhar**, **A.**, & Vaya, S. (2019). *Methods and systems for broadcasting targeted advertisements to mobile device*. US Patent 10,333,909.
7. **Dhar**, **A.**, Yu, D.-Y., & Capkun, S. (2019). *Integrity of user input in web pages*. EU Patent EP3477531A1.
8. 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.
9. 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.
10. **Dhar**, **A.**, & Yadav, K. (2018). *Methods and systems for providing non-auditory feedback to users*. US Patent App. 15/607,804.
11. 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, LaTeX
Tools/Frameworks	PyTorch, CUDA, Soot, Intel SGX, ARM TrustZone, ARM CCA
Web Dev	Html, css, JavaScript, Tomcat Web Server.