SHAILESH MISHRA

Fourth year PhD Student, School of Computer & Communication Sciences, EPFL

Email: shailesh.mishra@epfl.ch **Phone**: +41-0764723406

KEYWORDS

Security, Privacy, Digital Identities, Applied Cryptography

EDUCATION

École Polytechnique Fédérale de Lausanne *2022–Present*
PhD in School of Computer and Communication Sciences (IC)
Supervised by: Bryan Ford

Indian Institute of Technology, Kharagpur *2017–2022*
Bachelor's + Master's in Electrical Engineering CGPA: 9.03/10

RESEARCH EXPERIENCE

Privacy-preserving Self-Sovereign Identity Systems *Jan 2023–Present*
Supervised by **Prof. Bryan Ford** *Doctoral Assistant*, DEDIS, EPFL

- Working on developing building blocks for a privacy-preserving self-sovereign identity system with key recovery.
- *Apollo*: Proposed a new taxonomy for *recovery metadata management* to present the tradeoff between memorability burden and privacy in social vault recovery; built a novel framework for social vault recovery that minimizes memorability burden and maximizes privacy.
- *Privacy-preserving biometrics deduplication*: Building a decentralized biometric deduplication system for preserving the privacy of biometric templates in storage and computation.

Integration of Blockchain and IoT *Jan 2020–Oct 2021*
Supervised by **Prof. Raja Jurdak and Dr. Ali Dorri** *Remote Research Intern*, Queensland University of Technology

- Worked on implementing systems for making usage of blockchain with the internet of things scalable.
- *BlockTorrent*: Built an overlay network for off-chain communication in a system combining blockchain and BitTorrent.
- *Vericom*: Implemented an IoT-based blockchain to improve its performance by optimizing the number of packets shared.

Smart Contract Generation from Natural Language [Repository] *Feb 2020–Oct 2021*
Supervised by **Prof. Mohammad Hamdaqa** *Remote Research Intern*, Reykjavik University

- Built a chatbot using Xatkit and designed a domain-specific language to generate smart contract code.
- Integrated software engineering modules with language processing components for the code generation process.
- Performed a user study spanning diverse demographics to evaluate the chatbot's performance.

Blockchain Research & Development *Jun 2022–Aug 2022*
Supervised by **Michal Zajac, Joel Kahil and Marcos Maceo** *Engineering internship*, Nethermind

- Worked on designing identity system and analyzing cryptocurrencies respectively.
- *Research*: Designed an identity management system using blockchain and IPFS for operators in liquid staking.
- *Trantor*: Analyzed the various components of AAVE GHO and the performance of various stablecoins on AAVE.

AWARDS AND ACHIEVEMENTS

CYD Fellow	Awarded the Armasuisse CyberDefence (CYD) Doctoral Fellowship Program (2024-27).
KVPY Scholar	Selected for the KVPY fellowship by Department of Science and Technology, Govt. of India (2016).
SRFP Recipient	Selected for the SRFP fellowship programme by Indian Academy of Sciences (2019).

TALKS AND POSTER PRESENTATIONS

Talks

- IC3 Winter Retreat 2024, 2025
- CYD Cyber Alp Retreat 2024, 2025
- CYD Annual Conference 2024

Poster

- Summer Research Institute on Security and Privacy, EPFL 2024
- Swiss Federal Offices Day 2024

TEACHING ACTIVITIES

- Technology for Democratic Societies, Fall 2025, 2024
- Decentralized Systems Engineering, Fall 2025, 2023
- Advanced Topics on Privacy Enhancing Technologies, Spring 2025
- Fundamentals of Digital Systems, Spring 2024

STUDENT SUPERVISION

- Jose Pedro Costa Coelho, Master's Thesis, *TrueGraph: Graph-based Sybil Resistance through Proof of Personhood*
- Daniel Tavares Agostinho, Master's Thesis, *Mobile first digital assets mass-demand manage*
- Yago Perez, Semester Project, *Hint-enhanced Apollo*
- Tatiana Tuor, Semester Project, *Trust-enhanced Apollo*

VOLUNTEERING AND EXTRA-CURRICULAR ACTIVITIES

- **RAMP: Graduate Application Mentorship Program**
  - Initiated and managed a mentorship program where PhDs from EPFL help CS PhD applicants worldwide.
- **Member of EPIC (2022-2024)**
  - Helped in planning & organizing recreational activities for Computer Science PhDs at EPFL.
- **Tennis**
  - Inter-IIT probable in 2019 — one of the top 8 male tennis players in the institute.
  - Runner-up with RK Hall Tennis team among 12 teams in Inter-Hall Tennis Tournament, 2022.
- **Technology Head, RK Hall**
  - Guided over 80 undergraduate students as Captain of Product Design and OpenSoft Team in 2021-22.

SELECTED PUBLICATIONS (full publications list)

Apollo: Self-recovering Vault with Coercion Resistance. Mishra, S., Colombo, S., Tennage, P., Burkhart, M. & Ford, B. *Under preparation for submission.* [Preprint]

TRIP: Coercion-resistant Registration for E-Voting with Verifiability and Usability in Votegral. Merino, L.H., Colombo, S., Reyes, R., Azhir, A., Mishra, S., Tennage, P., Raeisi, M.A., Zhang, H., Allen, J.R., Tellenbach, B., Estrada-Galiñanes, V., & Ford, B. *ACM SIGOPS SOSP 2025* [Link]

ConsenStress: A Framework to Torture Test Consensus Protocols. Tennage, P., Mishra, S., Sonnino, A., Kokoris-Kogias, E., Jovanovic, P., & Ford, B. *EuroSys Poster, 2025* [Link]

iContractBot: A Chatbot for Smart Contracts' Specification and Code Generation. Qasse, I., Mishra, S., & Hamdaqa, M. *2021 IEEE/ACM Third International Workshop on Bots in Software Engineering (BotSE).* [Link]

Vericom: A Verification and Communication Architecture for IoT-based Blockchain. Dorri, A., Mishra, S., & Jurdak, R. *Ad Hoc Networks, Volume 133, 1 August 2022, 102882.* [Link]