Dmitrii Korobeinikov

Rochester, NY korobeinikov.net business.kdima@gmail.com linkedin.com/dmitrii-korobeinikov

Education

Computing and Information Sciences, Ph.D. 2025 --- present
Rochester Institute of Technology *Rochester, NY, USA*

- **Research topics:** Agentic AI for Testbeds, Federated Learning Security, Adversarial Attack Detection, Large-Scale Experimentation

Software Engineering, Master of Science 2022 --- 2025
Rochester Institute of Technology *(GPA 3.81)* *Rochester, NY, USA*

- **Subjects:** Software Architecture, Model-Driven Development, UML, Requirement Engineering, Quality Assurance, Networks, Web Applications, Algorithms, Object-Oriented Programming

Software Engineering, Bachelor of Science 2017 --- 2022
Peter the Great Polytechnic University *Saint-Petersburg, Russia*

- **Subjects:** Network Architecture, Database Management Systems Architecture, Software Development Methodologies, Neural Networks, Algorithms, Operating System Architectures, CPUs and Micro-controllers

Technical Skills

Languages: Python, Java, C++
ML & Data: PyTorch, Flower, Ray, NumPy, Pandas, Scikit-Learn, Hugging Face, LLMs, LoRA, OpenAI API, federated learning, anomaly detection, supervised/unsupervised learning, deep learning
Security: adversarial ML, model poisoning defenses, federated learning threat modeling, authentication hardening, network protocol analysis (HTTP, TCP/IP, DNS)
Backend & Data: aiohttp, Spring Boot, REST APIs, SQLAlchemy, Alembic, PostgreSQL, MySQL, SQLite
Infrastructure & Tools: AWS, Terraform, Docker, Linux, Bash, CUDA, SLURM/HPC, Git, GitHub Actions, CI/CD, pytest, Agile, JIRA
Frontend: React, TypeScript, Angular

Work Experience

Researcher of Video Summarization and Processing Pipelines May 2026 -- August 2026
North Carolina State University, Laboratory for Analytic Sciences

- Developing automated data collection and processing pipelines for real-time video content analysis, integrating Vision-Language models for semantic understanding and detection of structured events in unstructured media streams.

Lead Developer, *InteFL* Federated Learning Platform IEEE Intelligent Systems Feb 2024 --- Present
Rochester Institute of Technology, Data Quality Lab

- Lead development of InteFL, an open-source platform for designing, running and comparing federated learning experiments (26K lines of **Python**, 1,000+ commits); set the roadmap, review code, and coordinate 20+ contributors, including graduate capstone teams. github.com/dmitrykoro/fl-execution-framework
- Built the simulation engine on **Flower** and **Ray** with **PyTorch**: JSON-configured experiments across 25+ datasets (computer vision, medical imaging, NLP with **BERT/GPT-2 + LoRA**, time series), 20 Byzantine-robust aggregation strategies (Krum, Bulyan, FLTrust, FreqFed, …) and 5 data/model poisoning attacks, with reproducible runs on **CUDA** GPUs and **SLURM** clusters.
- Designed novel **anomaly detection** defenses against model poisoning, including **LQR-Fed**, which weights each client by solving a quadratic program every round; replaced the generic SLSQP solver with an exact $O(N \log N)$ solution.
- Built the experiment-tracking backend: **SQLAlchemy** models with **Alembic** migrations on **PostgreSQL**, a **SQLite** offline mode and a token-authenticated upload server; **2,400+ experiments** and 165+ compute hours recorded to date.
- Built an **aiohttp REST API** and a **React/TypeScript** web UI for launching runs, streaming logs and analyzing results, plus an **LLM agent (OpenAI API)** that turns natural-language requests into validated experiment configs.

Contributor at Summer Conference on Applied Data Science June 2025 -- July 2025
North Carolina State University, Laboratory for Analytic Sciences

- Designed and evaluated automated pipelines for temporal action retrieval within video summarization workflows using Vision-Language encoders; developed novel frame pre-processing techniques to improve detection precision and quantitative benchmark performance.

Teaching Assistant for Intelligent Security Systems Courses Aug 2024 --- Dec 2024
Rochester Institute of Technology, Department of Computer Science

- Contributed to a graduate course project on **federated learning security**, covering adversarial attack scenarios, trust-based anomaly detection, and countermeasure implementation. Mentored students in building ML-based threat detection modules, conducted code reviews, and guided debugging.

Backend Developer Sep 2021 --- Aug 2023
WEBIM Online Consulting Platform (A service similar to Zendesk, LiveAgent)

- Integrated **PostgreSQL** alongside **MySQL** for enhanced product flexibility, expanding deployment options by addressing limited database support. Utilized **Python 3.7--3.10**, **AIOHTTP**, and conducted extensive code refactoring, including resolving merge conflicts in 90+ files. Collaborated in a four-member development team.
- Hardened product security by redesigning authentication at service endpoints; implemented new identity verification algorithms across three backends with different architectures, including **PHP**. Collaborated with the deployment team for a new version release, introducing security-aware pipeline adjustments.
- Modified and improved external **HTTP APIs**, created custom chat and system logic in **Python** with **SQLAlchemy**, and optimized statistics metrics using **MySQL** and **PHP**.
- Actively engaged in determining technical requirements within **Agile** methodology using Atlassian tools (**JIRA**, **Confluence**), enhancing project efficiency and client satisfaction.

Academic Projects

AWS Cloud-Native Application for Live Stream Object Recognition | *Terraform*, *Rekognition*, *OpenCV*, *Django*, *SQLAlchemy*, *RabbitMQ*, *ffmpeg*

- Application utilizes advanced auto-scaling, message broker, cloud-native security and Infrastructure as Code (**IaC**) practices with **Terraform**. github.com/dmitrykoro/live-video-object-detection

IntelliMAD: a Framework for Secure Machine Learning Models Evaluation and Fine-tuning in Federated Setting | *Cybersecurity*

- Domain-agnostic framework for Federated Learning experiment management MS Thesis publication

Publications

D. Korobeinikov, R. Zatsarenko, S. Chuprov, A. Barea, and L. Reznik, "InteFL Framework: Optimizing Federated Learning with Metacognition for Application Design and Deployment," *IEEE Intelligent Systems*, Special Issue on Metacognitive Prediction of AI Behavior, 2026.

D. Korobeinikov, R. Zatsarenko, S. Chuprov, A. Barea, and L. Reznik, "InteFL: Framework for AI-Assisted Design of Trustworthy and Efficient Federated Learning Applications," in *Proceedings of the 2026 IEEE World Congress on Computational Intelligence (WCCI)*,

D. Korobeinikov, S. Chuprov, and L. Reznik, "Towards More Robust Federated Learning with Medical Imaging Model Anomaly Detection," in *2024 IEEE Western New York Image and Signal Processing Workshop (WNYISPW)*, 2024, pp. 1--4.

D. Korobeinikov, S. Chuprov, R. Zatsarenko, and L. Reznik, "Federated Learning Robustness on Real World Data in Intelligent Transportation Systems," in *19th Annual Symposium on Information Assurance (ASIA'24)*, Jun. 2024.

R. Zatsarenko, S. Chuprov, **D. Korobeinikov**, L. Reznik, and A. Peña, "MADE-PI: Framework for Effective Anomaly Detection in Federated Learning Applications," in *International Conference on Machine Learning and Applications (ICMLA)*, IEEE, 2025. [Accepted for publication]

S. Chuprov, **D. Korobeinikov**, R. Zatsarenko, and L. Reznik, "No Trust, No Learning? Improving Federated Learning Security and Robustness with Reputation and Trust," in *Data Science Workshop: From Theory to Practice*, 2025.

A. Narayanan, S. Chuprov, L. Reznik, R. Zatsarenko, and **D. Korobeinikov**, "Intelligent Soccer Event Detection and Highlights Generation with Broadcast Cues Integration," in *23rd IEEE International Conference on Machine Learning and Applications (ICMLA)*, 2024.

R. Zatsarenko, S. Chuprov, **D. Korobeinikov**, and L. Reznik, "Trust-Based Anomaly Detection in Federated Edge Learning," in *2024 IEEE World AI IoT Congress (AIIoT)*, May 2024, pp. 273--279.

S. Chuprov, R. Zatsarenko, **D. Korobeinikov**, and L. Reznik, "Robust Training on the Edge: Federated vs. Transfer Learning for Computer Vision in Intelligent Transportation Systems," in *2024 IEEE World AI IoT Congress (AIIoT)*, May 2024, pp. 172--178.

H. Patel, S. Chuprov, **D. Korobeinikov**, R. Zatsarenko, and L. Reznik, "Improving Federated Learning Security with Trust Evaluation to Detect Adversarial Attacks," in *19th Annual Symposium on Information Assurance (ASIA'24)*, Jun. 2024.

R. Zatsarenko, S. Chuprov, **D. Korobeinikov**, L. Reznik, and A. Peña, "How to Improve Federated Learning in Consumer Applications? Detect and Exclude Bad Clients," in *2026 IEEE 23rd Consumer Communications & Networking Conference (CCNC)*, IEEE, 2026, pp. 1--6.

R. Zatsarenko, S. Chuprov, **D. Korobeinikov**, L. Reznik, and A. Peredo, "Boosting Federated Model Convergence with Anomaly Detection and Exclusion."

Awards

Edmund S. Muskie Fellowship | *2024*

- culturalvistas.org/muskie

Fulbright Scholarship | *2023*

- us.fulbrightonline.org/about