

Sourasekhar Banerjee, Ph.D.

Postdoctoral Researcher, Department of Information Technology
Uppsala University, Sweden

sourasekhar.banerjee@it.uu.se | +46 730 987 453 | github.com/sourasb05 | [Google Scholar](#) | [LinkedIn](#)

RESEARCH INTERESTS

My research lies at the intersection of **federated learning**, **privacy-preserving machine learning**, and **distributed AI systems**, focusing on four theoretically grounded and practically validated themes:

- **Personalization and Heterogeneity:** Provably convergent FL algorithms that handle non-IID data and systems heterogeneity across large-scale distributed environments.
- **Continual Federated Learning:** Frameworks for adapting federated models to distributional shifts without catastrophic forgetting, applied to adaptive intrusion detection in IoT networks.
- **Trustworthy Federated Learning:** Quantifying and mitigating privacy leakage and adversarial threats in FL pipelines, with applications to verifiably secure distributed learning across IoT and cross-institutional settings. Also, explainability of the clients.
- **Explainable Federated Learning:** Privacy-preserving frameworks that attribute global model behavior to individual client contributions, turning FL into an auditable system that supports anomaly detection, fair valuation, and accountability in high-stakes domains.
- **Applied Federated Learning:** User-centric FL for continuous sensing environments, including cognitive health, image privacy, and cross-institutional collaboration under data scarcity.

EDUCATION

Ph.D. in Computing Science , Umeå University, Sweden <i>Thesis:</i> “Advancing Federated Learning: Algorithms and Use-Cases.” <i>Supervisors:</i> Assoc. Prof. Monowar Bhuyan; Prof. Erik Elmroth	2020 – 2024
M.Tech. in Computer Science & Engineering , University of Calcutta, India First Class; 82.83% <i>Thesis:</i> “A Framework Towards Generalized Mid-term Energy Forecasting Model for Industrial Sector in Smart Grid.” <i>Supervisor:</i> Prof. Nabendu Chaki	2016 – 2018
M.Sc. in Computer Science , University of Calcutta, India First Class; 75.54% <i>Thesis:</i> “A Design towards Reduced Message Complexity using Symmetric Algorithm for Process Synchronization.” <i>Supervisor:</i> Prof. Nabendu Chaki	2014 – 2016
B.Sc. in Computer Science (Hons.) , St. Xavier’s College, India First Class; 71%	2011 – 2014
Higher Secondary (WBCHSE) , Mahes Sri Ramkrishna Ashram Vidyalaya Passed; 81% (Best of Five)	2009 – 2011
Secondary (WBBSE) , Mahes Sri Ramkrishna Ashram Vidyalaya Passed; 82.75%	2009

RESEARCH EXPERIENCE

Postdoctoral Researcher <i>Department of Information Technology</i>	<i>Uppsala University, Sweden</i> Oct 2024 – Present
• Developed a domain continual learning-based intrusion detection system for RPL-IoT attack domains, evaluating catastrophic forgetting under distributional shift across heterogeneous IoT traffic. • Designing a domain continual learning framework for aggregation-free event-driven federated learning using knowledge distillation, to reduced catastrophic forgetting caused by spatio-temporal data heterogeneity in distributed IoT environments. (Ongoing) • Investigated the use of the MOMENT foundation model for multi-class attack identification in RPL-based IoT networks, demonstrating competitive attack detection and effective differentiation among Black-hole, DIS Flooding, Worst Parent, and Local Repair attacks. • Developed an LSTM-based intrusion detection system for RPL-based IoT networks that enhances attack detection by integrating TX/RX radio features with routing-layer features, achieving up to $\sim 4\%$ improvement in F1-score across DIS-Flooding, Local Repair, and Worst Parent attacks.	

- Developed FedLIME, a clustered federated learning method that groups clients by **LIME attribution (Explainability)** divergence instead of weight similarity. (Ongoing)

Research Intern

Institute of High Performance Computing

*A*STAR IHPG, Singapore*

Apr 2024 – Jun 2024

- Designed a **Federated Image Privacy Advisor** using personalized FL daisy-chaining, achieving a 30% improvement in privacy scoring accuracy over global FL baselines. Conducted multi-modal (text + image) FL experiments; compared privacy risks under global and personalized FL settings across multiple attack scenarios.

Doctoral Researcher

Department of Computing Science

Umeå University, Sweden

Jun 2020 – Sep 2024

- Authored and defended a PhD thesis covering personalized FL algorithms, feature selection, straggler mitigation, event-memorability and privacy risk prediction.
- Designed scalable personalized FL algorithms addressing statistical heterogeneity (non-IID distributions) with rigorous convergence analysis.
- Developed privacy risk prediction models quantifying per-client leakage as a function of model architecture and aggregation strategy.
- Built personalized FL models for **cognitive science** (event memorability prediction).

Research Fellow

Department of Computer Science & Engineering

IIT Patna, India

Aug 2018 – Jun 2020

- Designed an edge-deployable computer vision model for banned object detection in real-time.
- Delivered an embedded ML solution optimised for resource-constrained edge environments, resulting in a granted Indian patent.

PUBLICATIONS

Journal Articles

- [1] **Banerjee, S.**, Bhuyan, D., Elmroth, E., and Bhuyan, M. (2024). “Cost-Efficient Feature Selection for Horizontal Federated Learning.” *IEEE Transactions on Artificial Intelligence*, vol. 5, no. 12, pp. 6551–6565. [PDF]

Conference Papers

- [1] **Banerjee, S.**, Bergqvist, D., Toor, S., Rohner, C., and Johnsson, A. (2026). “Quantifying Catastrophic Forgetting in IoT Intrusion Detection Systems.” In *Proc. IEEE International Conference on Communications (ICC)*. [Preprint]
- [2] **Banerjee, S.**, Subramaniam, V., Roy, D., Subbaraju, V., and Bhuyan, M. (2026). “Personalized Image Privacy Advisors via Federated Daisy-Chaining.” In *Proc. IEEE/CVF Winter Conference on Applications of Computer Vision (WACV)*, pp. 2808–2817. [PDF]
- [3] **Banerjee, S.**, Roy, D., Subbaraju, V., and Bhuyan, M. (2025). “Predicting Event Memorability Using Personalized Federated Learning.” In *Proc. IEEE/CVF Winter Conference on Applications of Computer Vision (WACV)*, pp. 1556–1565. [PDF]
- [4] Dadras, A., **Banerjee, S.**, Prakhya, K., and Yurtsever, A. (2024). “Federated Frank-Wolfe Algorithm.” In *Proc. Joint European Conference on Machine Learning and Knowledge Discovery in Databases (ECML-PKDD)*, pp. 58–75. Springer. [PDF]
- [5] **Banerjee, S.**, Dadras, A., Yurtsever, A., and Bhuyan, M. (2024). “Personalized Multi-tier Federated Learning.” In *Proc. International Conference on Neural Information Processing (ICONIP)*, pp. 192–207. Springer. [PDF] (*Early version presented at FL-NeurIPS Workshop, 2022.*)
- [6] **Banerjee, S.**, Patel, Y. S., Kumar, P., and Bhuyan, M. (2023). “Towards Post-disaster Damage Assessment using Deep Transfer Learning and GAN-based Data Augmentation.” In *Proc. 24th International Conference on Distributed Computing and Networking (ICDCN)*, pp. 372–377. ACM. [PDF]
- [7] **Banerjee, S.**, Vu, X.-S., and Bhuyan, M. (2022). “Optimized and Adaptive Federated Learning for Straggler-Resilient Device Selection.” In *Proc. International Joint Conference on Neural Networks (IJCNN)*, pp. 1–9. IEEE. [PDF]
- [8] **Banerjee, S.**, Elmroth, E., and Bhuyan, M. (2021). “Fed-FiS: A Novel Information-Theoretic Federated Feature Selection for Learning Stability.” In *Proc. International Conference on Neural Information Processing (ICONIP)*, pp. 480–487. Springer. [PDF]

- [9] **Banerjee, S.**, Misra, R., Prasad, M., Elmroth, E., and Bhuyan, M. (2020). “Multi-diseases Classification from Chest X-ray: A Federated Deep Learning Approach.” In *Proc. Australasian Joint Conference on Artificial Intelligence (AI 2020)*, pp. 3–15. Springer. [PDF]
- [10] Patel, Y. S., **Banerjee, S.**, Misra, R., and Das, S. K. (2020). “Low-Latency Energy-Efficient Cyber-Physical Disaster System Using Edge Deep Learning.” In *Proc. 21st International Conference on Distributed Computing and Networking (ICDCN)*, pp. 34:1–34:6. ACM. [PDF]
- [11] Chakraborty, M., **Banerjee, S.**, and Chaki, N. (2020). “A Framework Towards Generalized Mid-term Energy Forecasting Model for Industrial Sector in Smart Grid.” In *Proc. International Conference on Distributed Computing and Internet Technology (ICDCIT)*, pp. 296–310. Springer.
- [12] **Banerjee, S.**, Mukherjee, P., Kanrar, S., and Chaki, N. (2018). A novel symmetric algorithm for process synchronization in distributed systems. In *Algorithms and Applications: ALAP 2018* (pp. 51-66). Singapore: Springer Singapore. [PDF]

Patent

- [1] Shekhar, H., **Banerjee, S.**, Misra, R., and Patel, Y. S. (2024). “System and Method for Detection of Banned Objects from Images in Real-time using Intelligence at the Edge.” Indian Patent No. 550543, Application No. 202031006618.

Book Chapters

- [1] **Banerjee, S.**, Ghosh, S., and Mishra, B. K. (2021). Application of deep learning for energy management in smart grid. In *Deep Learning in Data Analytics: Recent Techniques, Practices and Applications* (pp. 221-239). Springer.

Workshop

- [1] Lunderbye, E., **Banerjee, S.**, Rohner, C., and Johnsson, A. (2026). “Towards Intrusion Detection Systems for RPL-based IoT Networks using Foundation Models.” Accepted and presented in the Swedish National Computer Networking Workshop (SNCNW), arXiv preprint arXiv:2606.03530.
- [2] Sun, Y., Johnsson, A., and **Banerjee, S.** (2026). “Rethinking IoT Intrusion Detection: Augmenting Routing Metrics with Radio Features.” Accepted and presented in the Swedish National Computer Networking Workshop (SNCNW), arXiv preprint arXiv:2606.07282.
- [3] **Banerjee, S.**, Yurtsever, A., and Bhuyan, M. (2022). “Personalized Multi-tier Federated Learning,” Accepted and presented in Workshop on Federated Learning: Recent Advances and New Challenges (in Conjunction with NeurIPS 2022).

PEDAGOGICAL TRAINING

Academic Teacher Training Course

Uppsala University, Sweden

Unit for Academic Teaching and Learning

Autumn 2025

- Completed a university-level teacher training course covering curriculum design, constructive alignment, formative and summative assessment, inclusive teaching strategies, research-based teaching, and digital learning environments.
- **Project:** “Responsible Integration of LLMs in Higher Education”

TEACHING EXPERIENCE

Teacher

Uppsala University, Sweden

Department of Information Technology

Period III: Jan–Mar 2025, Jan–Mar 2026

- *Information Technology and Energy Storage.* [course link]
- Delivered lectures, tutorials, and assignments covering theoretical foundations of machine learning and data-driven applications in battery management systems.

Teaching Assistant

Umeå University, Sweden

Department of Computing Science

Period III: Jan–Mar 2022, Jan–Mar 2023

- *Operating Systems* (2022, 2023).
- Delivered tutorials and lab sessions reinforcing core OS concepts including process management, memory allocation, scheduling, and kernel programming.

STUDENT SUPERVISION

Master’s Thesis Supervision

- “Machine Learning for Cybersecurity in Internet of Things Networks.” — Yichang Sun [2026] (*Ongoing*)

Bachelor's Thesis Supervision

- “Benchmarking Federated Learning Algorithms for Intrusion Detection in RPL-IoT networks” — Robin Forslund [2026] (*Completed*)
- “An Investigation into Intrusion Detection System Generalisation Against Novel Attacks” — Max Dahlgren [2026] (*Completed*)
- “Intrusion Detection System Generalisation in IoT Blackhole Attacks” — Oskar Nylin [2025] (*Completed*)
- “Assessing the Generalizability and Scalability of an IoT Intrusion Detection System against DIS-Flooding Attack Variants” — Hans-Eskil Ytterfelt Martinsson [2025] (*Completed*)

COMPETITIVE GRANTS & FUNDING

- **Research Internship Grant** (110,000 SEK) — A*STAR IHPC, Singapore. Awarded by the Wallenberg AI, Autonomous Systems and Software Program (WASP), 2024.
- **Travel Grant** (\$500 USD) — IEEE World Congress on Computational Intelligence (WCCI), 2022.

PROFESSIONAL SERVICE

Peer Review

- *Conferences*: NeurIPS, ICML, AAAI, ICLR, AISTATS, ICONIP, IJCNN, ACSS.
- *Journals*: IEEE TAI, IEEE TCSS, Sensors, MDPI.

Invited Talks

- Industry & Research: Ericsson Research Sweden (2025); NTU Singapore (2023); A*STAR IHPC Singapore (2023, 2024); Scaleout AB Uppsala (2025)
- Faculty Development Programs: SRM University (2025, 2026); NIT Delhi (2025); NIT Warangal (2025); IIIT Gwalior (2025)

TECHNICAL SKILLS

- **Federated Learning Frameworks**: FEDn, Flower, and NVIDIA FLARE
- **ML / Data Science**: Federated Learning, Continual Learning, Personalised ML, Statistical Optimisation, Feature Selection, Predictive Modelling, Time-Series Modelling, Multi-modal Analysis, Anomaly Detection, Privacy-Preserving AI
- **Deep Learning**: CNN, LSTM, GAN, VAE, Transformers, Autoencoder, Diffusion Models
- **GenAI / LLM**: RAG, vector database, Agentic AI, Fine-tuning, LORA/PEFT
- **Data Science Stack**: Python, PyTorch, scikit-learn, pandas, NumPy, Matplotlib, Seaborn, SQL
- **MLOps / DevOps**: Docker, Kubernetes, Git, GCP, Azure
- **Programming Languages**: Python, JAX, C/C++, Java