Aradhika Bagchi

Edinburgh, UK
A.D.Bagchi@sms.ed.ac.uk • linkedin.com/in/aradhika-bagchi

EDUCATION

University of Edinburgh **Edinburgh, UK**
PhD in Informatics, UKRI CDT in Machine Learning Systems **Sep 2025 – Present**
Advisor: Professor Tariq Elahi
Fully funded by UK Research and Innovation (UKRI)
Relevant Courses: Machine Learning Systems, Privacy-Preserving Machine Learning

Columbia University **New York, NY**
MS in Computer Science, Advanced Research Track **Sep 2022 – May 2024**
Advisor: Professor Steven M. Bellovin
Relevant Courses: Intrusion Detection Systems; Cybersecurity: Tech, Policy, Law; Speech Recognition; Natural Language Processing; Security II; Policy for Privacy Technologies; Analysis of Algorithms; Anonymity and Privacy

Cardiff University **Cardiff, UK**
BSc in Computer Science, First Class Honours **Oct 2018 – Jun 2021**
Relevant Courses: Large-Scale Databases, Forensics, Object-Orientation, Algorithms and Data Structures, Cybersecurity, Human-Computer Interaction

TECHNICAL SKILLS

Programming: Python, Java, C++, SQL, MATLAB, HTML/CSS
ML & Frameworks: PyTorch, TensorFlow, Hugging Face Transformers, scikit-learn, NumPy, Pandas, Kaldi, BERT, GANs, Opacus
Tools & Infra: Git, Linux, SLURM / HPC clusters, AWS, LaTeX, Flask, Django, MySQL, MongoDB
Other: Research, technical writing, communication, teamwork, agile project management

RESEARCH EXPERIENCE

University of Edinburgh **Edinburgh, UK**

Privacy-Preserving Age Verification from Facial Embeddings – advised by Prof. Tariq Elahi
Sep 2025 – Present

- Designing a privacy-preserving pipeline that transforms facial embeddings into representations specialised for age prediction while suppressing sensitive attributes (identity, gender, ethnicity).
- Combining a learned bottleneck that restricts information flow, adversarial training that discourages recovery of protected attributes, and calibrated differential privacy noise applied to the latent representation for formal guarantees.
- Adapting the CPGAN adversarial training loop to operate over SwinFace embeddings; using gradient-based sensitivity analysis to identify which dimensions encode age and applying selective DP noise via a learned mask.
- Formalising a threat model with an honest-but-curious model owner, a privacy intermediary in a TEE, and potentially dishonest users, alongside a verification service for auditing correctness. Motivated by the UK Online Safety Act.

Columbia University **New York, NY**

Differential Privacy Algorithms in Sensitive Datasets – advised by Prof. Steven M. Bellovin
Jan 2023 – May 2024

- Studied the efficacy of the Laplace mechanism in protecting sensitive kindergarten immunisation data across demographically diverse Californian counties.
- Analysed re-identification risks under differential privacy, comparing performance in diverse vs. homogeneous populations; used Chi-Squared tests to evaluate vulnerability when DP-protected data is combined with non-private datasets.
- Co-authored research with Prof. Bellovin proposing context-sensitive privacy frameworks for equitable protection of marginalised communities.

NLP Sentiment Analysis on Crime and Climate Data – advised by Prof. Sharon Di
May 2023 – Sep 2023

- Built a custom Python web scraper to collect large-scale social media data; preprocessed and fine-tuned BERT for sentiment classification.
- Owned the full ML pipeline (preprocessing, feature engineering, training, evaluation) and used statistical methods to quantify correlations between subway crime rates and climate-change sentiment.

Legal and Privacy Concerns with Voice-Activated Virtual Assistants – advised by Prof. Homayoon Beigi

Oct 2022 – Dec 2022

- Analysed privacy risks in voice-activated assistants across ASR, ML, and NLP stages; examined Fourth Amendment and GDPR implications and proposed mitigations in a six-page IEEE-style report.

Cardiff University **Cardiff, UK**

Undergraduate Thesis: Systems Modelling of COVID-19 Impact on NHS Cancer Services

Sep 2020 – Dec 2020

- Developed an AnyLogic-based systems model of NHS cancer services during the pandemic, identifying critical bottlenecks and producing evidence-based policy recommendations.

PUBLICATIONS

1. D. Beechey, J. Bobolz, **A. Bagchi**, and T. Elahi. *A Closer Look at Abuse Prevention and Metadata Privacy in Interoperable E2EE Messaging.* In submission to the 33rd ACM Conference on Computer and Communications Security (ACM CCS 2026).

TEACHING EXPERIENCE

University of Edinburgh **Edinburgh, UK**

Teaching Assistant – Computer Security **Sep 2025 – Dec 2025**

- Supported grading of the undergraduate and graduate Computer Security course (cryptographic primitives, authentication, network and systems security).
- Ran tutorials and labs, graded coursework, and held office hours.

Columbia University **New York, NY**

Teaching Assistant II – COMS E6998: Fundamentals of Speech Recognition **Sep 2023 – Dec 2023**

- Co-designed the course schedule with Prof. Homayoon Beigi; supported training on the Kaldi toolkit and the TED-LIUM corpus.
- Ran weekly office hours, graded assignments and exams, and gave research project guidance to 20 graduate students.

Teaching Assistant – COMS 4419: Internet Technology, Economics and Public Policy **Sep 2022 – Dec 2022**

- Graded assignments, proctored midterms, and held office hours for Prof. Henning Schulzrinne's interdisciplinary course.

Cardiff University **Cardiff, UK**

Undergraduate Teaching Assistant **Sep 2020 – Dec 2020**

- Delivered tutorials for CM1103: Problem Solving with Python and CM1208: Mathematics for Computer Science to a class of 200 students.