Harsh Kasyap

Machine Learning (Security)

ℹ 15 January 1994

☎ +91 7276393663

✉ hkasyap.cse@iitbhu.ac.in
harsh.kasyap@warwick.ac.uk
harshkasyap@gmail.com

in harsh-kasyap

🌐 harshkasyap.github.io

Skills

Languages: Python, Java, C, C++

Lib/Frameworks: Scikit-learn, TensorFlow, PyTorch, PySyft

Databases: MongoDB, SQL

DevOps: Jenkins, Nuget, Maven, Gradle, Cloud, Wix, GIT, JIRA

Cloud: Amazon AWS EC2, VPC, Managed-Blockchain

Accomplishments

DST Inspire Faculty Fellowship, India | (2025-2030)

Privacy Enhancing Technology Symposium Travel Award, UK | 2024

IEEE SaTML Travel Award | 2023

EO Global Student Entrepreneur Awards Kolkata Finalists | 2022

Runner-up in the National Level VJ Hacathon-Victory & Joy in Smart Innovations under the domain of Agriculture | Oct'21 | VNR VJIET

Awarded for Most Promising Student of Computer Department | July'16 | V.I.I.T Pune

First in Fourth and Third Year of Computer Engineering | July'16 | V.I.I.T Pune

First and Runner-up in multiple project competitions.

Oracle Certified Java SE 6 Programmer

ATAL FDP on Cyber Security and Cryptography | IIITDM K, India

GAIN Course on Distributed Systems and Machine Learning | IIT Patna

Work Experience

Since Jul'25 **Assistant Professor** Indian Institute of Technology (BHU) Varanasi, India

- Teaching Responsibilities in the Department of Computer Science and Engineering.
- Researcher in private data sharing and privacy-preserving machine learning, Trustworthy AI.

Dec'23-Jul'25 **Research Associate** The Alan Turing Institute, London, UK

- Involved in FAIR (Framework for responsible adoption of artificial intelligence in the financial services industry) and TDI (Trustworthy Digital Identity) Projects, for developing fair private, robust and veirfiable collaborative machine learning.
- Privacy preserving fuzzy matching for name, biometrics, etc.
- Development of Post Quantum Group Signature for EPIDs.

Sep'24-Mar'25 **Research Associate** The University of Warwick - WMG, UK

- Researcher in Secure Cyber Systems Research Group (SCSRG).
- Working on private information sharing and collaborative learning in edge AI-empowered connected autonomous vehicles and vehicle platooning.

Jul'23-Nov'23 **Research Assistant** The Alan Turing Institute, London, UK

- Researcher in FAIR Project under privacy and security theme.
- Working on Secure Data Sharing across borders with HSBC.

Jan'19-Nov'23 **Research Scholar** Indian Institute of Technology Patna, India

- Worked on privacy and security threats in Federated Learning.
- Teaching Associate for Blockchain | Cryptography | PL | HL.

Aug'16-Jan'19 **Software Engineer** Diebold Nixdorf, Mumbai, India

- Worked on Mobile, Card-less and Contact-less Transactions.
- Designed CI/CD Solutions for ATM VISTA Project.

Other Associations

Feb'24-Jan'27	**Honorary Research Fellow**	The University of Warwick - WMG, Coventry, UK.
ECAI 2024,25	**Program Committee**	27th,28th European Conference on Artificial Intelligence.
Since Jan'24	**Member, IEEE**	
Jan'21-Jan'23	**Student Member, IEEE**	
Nov'20-Jan'22	**Treasurer, IEEE Student Branch**	Indian Institute of Technology Patna, India.
Feb'21-Jul'21	**Post Graduate Representative**	Indian Institute of Technology Patna, India.

Research Interests

- **Artificial Intelligence**
  Machine Learning;
  Federated (collaborative machine) Learning;
  Privacy-preserving ML;
  Trustworthy AI;
  Generative AI;
  AI in Engineering
- **Computer Security**
  Data Privacy;
  Private Set Intersection;
  Homomorphic Encryption;
  Multi-Party Computation;
  Zero-Knowledge Proofs;
  Post-Quantum Crypto;
  Blockchain
- **AI for Science**
  Scientific Foundation Models;
  Privacy-Preserving Scientific Data Analysis;
  AI for Biomedical;
  Interpretability and Explanability in Decisions

Education

Jan'19-Dec'23	**Ph.D.**	Computer Science and Eng., Indian Institute of Technology Patna, India.
Nov'23-Dec'23	**Visiting Research Student, Ph.D.**	WMG, University of Warwick, Coventry, UK.
Aug'12-Jun'16	**B.E.**	Vishwakarma Institute of Information Technology Pune, Pune Univ., India.
May'09-May'11	**Senior and Higher Secondary**	Kendriya Vidyalaya Kankarbagh, Patna, India.

Teaching Services

- **CSO101: Computer Programming.** Undergraduate core course covering C programming fundamentals, problem solving, and algorithmic thinking. Jul'25, Jan'26.
- **CS314: Powers of AI.** Undergraduate elective introducing foundations and capabilities of AI. Jan'26.

Academic Services

1. Co-organiser, **Two-Day Faculty and Research Scholars Immersion Workshop on Discovering AI's Application Landscape**, IIT (BHU) Varanasi, January 14–15, 2026. Focused on applying AI/ML to interdisciplinary problems in engineering and life sciences and enabling collaborative problem formulation.
2. Co-organiser, **Research Scholar AI Workshop**, IIT (BHU) Varanasi, December 22–23, 2025. Featured spotlight talks and collaborative activities to design and solve real-world problems using AI.
3. Organizer, **Federated HPC Workshop**, MIT Bangalore, Dec 12, 2025 — focused on scalable federated learning and high-performance computing.

Selected Publications

1. **Harsh Kasyap**, Minghong Fang, Zhuqing Liu, Carsten Maple, Somanath Tripathy, **Fairness-Constrained Optimization Attack in Federated Learning.** IEEE TrustCom 2025. `https://arxiv.org/abs/2510.12143`.
2. Yalan Wang, Bryan Kumara, **Harsh Kasyap**, Liqun Chen, Sumanta Sarkar, Christopher J.P. Newton, Carsten Maple, Ugur Ilker Atmaca, **BACON: An Improved Vector Commitment Construction with Applications to Signatures.** IEEE TrustCom 2025. `https://eprint.iacr.org/2025/1411`.
3. **Harsh Kasyap**, Ugur Atmaca, Carsten Maple, Graham Cormode, Jiancong He, **Privacy-preserving Fuzzy Name Matching for Sharing Financial Intelligence.** `https://arxiv.org/abs/2407.19979`.
4. **Harsh Kasyap**, Ugur Atmaca, Carsten Maple, **Private Fairness-aware Aggregation in Federated Learning for Financial Fraud Detection (Extended Abstract).** International Conference on AI and the Digital Economy (CADE 2025). `https://ieeexplore.ieee.org/document/11197619`.
5. **Harsh Kasyap**, Ugur Atmaca, Michela Iezzi, Toby Walsh, Carsten Maple, **Mitigating Bias: Model Pruning for Enhanced Model Fairness and Efficiency.** 27^{th} European Conference on Artificial Intelligence, ECAI 2024. `https://ebooks.iospress.nl/doi/10.3233/FAIA240589`.
6. **Harsh Kasyap**, Ugur Atmaca, Carsten Maple, **Privacy-preserving personalised federated learning financial fraud detection (Extended Abstract).** International Conference on AI and the Digital Economy (CADE 2024). `https://ieeexplore.ieee.org/abstract/document/10700884/`.
7. **Harsh Kasyap**, Somanath Tripathy, **Sine: Similarity is not enough for mitigating Local Model Poisoning Attacks in Federated Learning.** IEEE Transactions on Dependable and Secure Computing, 2024, `https://doi.org/10.1109/TDSC.2024.3353317`.
8. **Harsh Kasyap**, Somanath Tripathy, **Privacy-preserving and Byzantine-robust Federated Learning Framework using Permissioned Blockchain.** Expert Systems with Applications, 2023, `https://doi.org/10.1016/j.eswa.2023.121192`.
9. **Harsh Kasyap**, Somanath Tripathy, **Beyond data poisoning in federated learning.** Expert Systems with Applications, Elsevier, 2023, `https://doi.org/10.1016/j.eswa.2023.121192`.
10. **Harsh Kasyap**, Somanath Tripathy, Mauro Conti, **HDFL: Private and Robust Federated Learning using Hyperdimensional Computing.** 22^{nd} IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), 2023.
11. **Harsh Kasyap**, Arpan Manna, Somanath Tripathy, **An Efficient Blockchain assisted Reputation aware Decentralized Federated Learning Framework.** IEEE Transactions on Network and Service Management (TNSM), 2022, `https://doi.org/10.1109/TNSM.2022.3231283`.
12. **Harsh Kasyap**, Somanath Tripathy, **Hidden Vulnerabilities in Cosine Similarity based Poisoning Defense.** 56^{th} Annual Conference on Information Sciences and Systems, 2022, `https://doi.org/10.1109/CISS53076.2022.9751167`.
13. Arpan Manna, **Harsh Kasyap**, Somanath Tripathy, **Moat: Model Agnostic Defense against Targeted Poisoning Attacks in Federated Learning.** 23^{rd} International Conference on Information and Communications Security (ICICS), 2021, `https://doi.org/10.1007/978-3-030-86890-1_3`.
14. **Harsh Kasyap**, Somanath Tripathy, **Privacy-preserving decentralized learning framework for healthcare system.** ACM Transactions on Multimedia Computing, Communications, and Applications (TOMM), 2021, `https://doi.org/10.1145/3426474`.

Books

Somanath Tripathy, **Harsh Kasyap**, Minghong Fang, **Federated Learning: Security and Privacy.** CRC Press / Routledge (1st Ed.), 2026. ISBN 9781041174622. https://www.routledge.com/Federated-Learning-Security-and-Privacy/Tripathy-Kasyap-Fang/p/book/9781041174622.

https://scholar.google.com/citations?user=1kGoXAUAAAAJ&hl=en

International Research Collaborations and Consortia

1. **Trustworthy AI for All** (RAI UK Collaboration Scheme), 2026. *Partner Institution: Indian Institute of Technology (BHU) Varanasi*. An international consortium led by the University of Warwick, involving NTU Singapore, EPFL, CMU, Tel Aviv University, IIT Bombay, University of Glasgow, and others. Contribution towards research on **trustworthy AI, AI governance, and digital public infrastructure**.

2. **Mathematical Algorithms for Privacy-Preserving AI to Combat Global Scams** (NTU–Warwick Joint Seed Fund), 2026. *Role: International Collaborator (IIT BHU)*. Joint research initiative between the University of Warwick and Nanyang Technological University focusing on **federated learning and fully homomorphic encryption** for privacy-preserving scam detection.

Funded Research Projects

AI-enabled Indigenous Contactless Multimodal Biometric System **(Principal Investigator)**

Uttar Pradesh Electronics Corporation Ltd. (UPEIDA), Government of Uttar Pradesh

Duration: 2026–2027 **Total Funding:** INR 40 Lakhs

Design and development of an **AI-driven, contactless multimodal biometric authentication system** for **secure defence access control and battlefield surveillance**. The project focuses on building an **indigenous, scalable, and resilient identity verification framework** by integrating **multimodal biometric sensors**, **edge AI devices**, and **UAV-assisted surveillance platforms**.

DST INSPIRE Faculty Fellowship **(Principal Investigator)**

Department of Science and Technology (DST), Government of India

Duration: 2025–2030 **Funding:** INR 7 Lakhs per year

Independent research programme on **Trustworthy and Privacy-Preserving Machine Learning**. The project focuses on designing secure, robust, fair, and verifiable collaborative learning frameworks, with particular emphasis on **Federated Learning** and **Privacy-Enhancing Technologies** (Homomorphic Encryption, Secure MPC, Differential Privacy, Zero-Knowledge Proofs). It aims for real-world deployments for use cases in sensitive applications, particularly in **finance**.

Invited Talks

- "Privacy-preserving (Collaborative) Machine Learning" at IndoML ECR Forum, December 21, 2025, online.
- "Privacy-preserving Federated Learning for UAV-assisted Applications" at PES University, December 17, 2025, India.
- "The Secret Behind Privacy-Friendly Machine Learning" at Coding Ninjas Online Platform, December 14, 2025, online.
- "Privacy-preserving (Collaborative) Machine Learning" at FDP organised by REC Sonbhadra, December 8, 2025, India.
- "Privacy-preserving Machine Learning" at Indo–Japan Symposium, November 18, 2025.
- "Federated Learning: Privacy, Robustness and Fairness" at FDP organised by the Department of CSE and School of Sciences (Mathematics), IIITDM Kancheepuram, July 22, 2025, online.
- "Privacy-preserving Fairness-aware Machine and Federated Learning" at the Centre for Computer Networks and Cyber Security, PES University, March 25, 2025, online, https://youtu.be/Qqkt34A4BvI.
- "Private and Secure Fuzzy Name Matching" at FHE.org Meetup, October 10, 2024, online, https://fhe.org/meetups/059-Private_and_Secure_Fuzzy_Name_Matching.
- "Federated Learning: Privacy-Preserving (Collaborative) Machine Learning" at the Centre for Computer Networks and Cyber Security, PES University, January 17, 2024, online, https://youtu.be/adpZziC7M1k.