Harsh Kasyap

Machine Learning (Security)

15 January 1994

+91 7276393663
+44 7774919377

harsh.kasyap@warwick.ac.uk
hkasyap@turing.ac.uk
harshkasyap@gmail.com

harsh-kasyap

harshkasyap.github.io

Skills

Languages: Python, Java, C, C++

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

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.

Certifications

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.

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** 27^{th},28^{th} 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
  - Collaborative Learning
  - Federated Learning
  - Machine Learning Security
  - Privacy-preserving ML
  - Trustworthy AI
- **Computer Security**
  - Data Privacy
  - Private Set Intersection
  - Homomorphic Encryption
  - Secure Multi-Party Comp.
  - Zero Knowledge Proofs
  - Post Quantum Cryptography

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.

Other Activities

- Reviewer in Peer-Reviewed Journals in IEEE, Elseiver and Springer (IEEE TIFS, TDSC, IEEE Internet Computing, Expert Systems with Applications, etc.)
- Co-ordinated 17^{th} International Conference on Information Systems Security (ICISS) in IIT Patna | 2021

Invited Talks

- "Privacy preserving Fairness aware Machine and Federated learning" organised by the Centre for Computer Networks and Cyber Security (PES University) on 26th March, 2025, online, https://youtu.be/Qqkt34A4BvI.
- "Private and Secure Fuzzy Name Matching" organised by FHE.org on Oct 10th, 2024, online, https://fhe.org/meetups/059-Private_and_Secure_Fuzzy_Name_Matching
- "Federated Learning: Privacy-Preserving (Collaborative) Machine Learning" organised by the Centre for Computer Networks and Cyber Security (PES University) on 17th January, 2024, online, https://youtu.be/adpZziC7M1k.

Selected Publications

1. **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.
2. **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). Accepted.
3. **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.
4. **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/.
5. **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.
6. **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.
7. **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.
8. **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.
9. **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.
10. **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.
11. Debasmita Manna, **Harsh Kasyap**, Somanath Tripathy, **MILSA: Model Interpretation Based Label Sniffing Attack in Federated Learning.** International Conference on Information Systems Security (ICISS), 2022, https://doi.org/10.1007/978-3-031-23690-7_8.
12. Sanjay Murmu, **Harsh Kasyap**, Somanath Tripathy, **PassMon: A Technique for Password Generation and Strength Estimation.** Journal of Network and Systems Management, 2021, https://doi.org/10.1007/s10922-021-09620-w.
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. Parth Parag Kulkarni, **Harsh Kasyap**, Somanath Tripathy, **DNet: An efficient privacy-preserving distributed learning framework for healthcare systems.** 23^{rd} International Conference on Information and Communications Security (ICICS), 2021, https://doi.org/10.1007/978-3-030-86890-1_3.
15. **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.

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

Academic and Industrial Projects

FAIR **Responsible artificial intelligence in financial services**

The Alan Turing Institute (In collaboration with HSBC) | 2024-25

Functionalities

1. Privacy, Integrity, Verifiability in collaborative machine learning.
2. Developing a private and secure fuzzy name matching scheme to find approximate similar names between two organizations across borders.

Role

1. Integrating Robust aggregation rules with PETs.
2. Ensuring the integrity of local and global model updates.
3. Developing Secure Protocol for Approximate Entity Resolution.

Technologies

1. Federated Learning
2. PETs: HE, SMPC and DP

TDI **Trustworthy Digital Identity**

The Alan Turing Institute (Funded by Bill and Melinda Gates Foundation) | 2024-25

Functionalities

1. Investigate and mitigate the technical, social, and other risks of digital identity and contribute towards the development of more trustworthy systems.

Role

1. Developing a private and fair biometric data sharing scheme.

Technologies

1. PETs: HE, SMPC
2. Machine Learning: Fairness

DevOps **Continuous Integration and Development** DN | 2018

Functionalities

1. Automate Build, Testing and Packaging Pipelines.
2. Automatic Error Reporting and Maintenance Scripts for Builds.
3. Migrate Source Code to GIT (BitBucket).

Role

1. Designed and Created Small Repositories for faster build.
2. Created Jenkins Pipeline for each of the Repository.
3. Prepared Scripts for creating modular and testable artifacts.

Technologies

1. GIT, Phoenix PTC (Source Code Management)
2. Jenkins (Automation Server) and Nexus (For Artifact Storage)
3. WIX (MSI Generation, Scripts written for custom use)
4. Maven, Gradle, Nuget (Resolving Dependencies)

NFC EMV **Contact Less ATM Transactions** DN | 2018

Functionalities

1. Contactless card transactions, called NFC-EMV transactions.
2. End-to-end secure Atm transactions.
3. Ensuring EMV implementation for secure transactions.

Role

1. Application Layer Design.
2. Device Layer Interaction with Application.
3. Communication with Host as per EMV Protocols.

Technologies

1. C++, Angular, HTML, CSS
2. Speech Engines, Skype, ATM Emulation Software's

1:1 Ad **Targeted Marketing Ads** DN | 2017

Functionalities

1. ATM Marketing Ads based on customer personalized profiles.
2. Different ads classification based on nature of the customer.
3. Cloud Service Integration of the Marketing Ads with ATMs.

Role

1. Designing and implementing Application UI.
2. Support Region, bank and customer classification.
3. Responsive Design for Different Atm Resolutions.

Technologies

1. C++, Angular, HTML, CSS