Umesh Kashyap

✉ umeshk@iitbhilai.ac.in ☎ +91-8889649525 Bhilai, India LinkedIn GitHub Google Scholar

PROFILE SUMMARY

Ph.D. Scholar at the **Indian Institute of Technology (IIT) Bhilai** with 4+ years of research experience in **Trustworthy AI** and **Adversarial Machine Learning**. Specialized in developing robust defense mechanisms against adversarial attacks, perceptual privacy protection, and deepfake detection.

Proven track record of publishing in high-impact venues (IEEE Transactions, SPACE) and securing competitive research funding (TIH Fellowship, NFOBC). Seeking a Post-Doctoral position to leverage expertise in secure deep learning architectures and contribute to cutting-edge research in AI safety.

EDUCATION

Ph.D. in Computer Science (Ongoing) *2022 - Present*
Indian Institute of Technology Bhilai, India
Thesis Focus: Adversarial Security Evaluation & Privacy-Preserving Deep Learning

M.Sc. Computer Science *2018 - 2020*
Atal Bihari Vajpayee University, Bilaspur, India

B.Sc. Computer Science *2015 - 2018*
Bilaspur University, Bilaspur, India

RESEARCH INTERESTS

- **Adversarial Machine Learning:** Attacks (Patch, Gradient-based) and Defense mechanisms.
- **Privacy-Preserving AI:** Perceptual encryption, secure inference, and data privacy.
- **Forensics:** Deepfake detection, attribution, and style-based anomaly detection.
- **Trustworthy AI:** Robustness evaluation and model security benchmarking.

PUBLICATIONS

1. R. Kumar, **U. Kashyap**, S. S. Ali, *"Gradient-Guided Adversarial Patch Attack for Deep Neural Networks."* **International Conference on Security, Privacy, and Applied Cryptography Engineering (SPACE)**, pp. 227–245, 2026.
2. **U. Kashyap**, S. K. Padhi, S. S. Ali, *"Is Perceptual Encryption Secure? A Security Benchmark for Perceptual Encryption Methods."* **IEEE Transactions on Artificial Intelligence**, 2025.
3. A. Vishwakarma, **U. Kashyap**, S. S. Ali, *"Adversarial Malware Detection."* **International Conference on Security, Privacy, and Applied Cryptography Engineering (SPACE)**, pp. 277–286, 2024.
4. S. K. Padhi, H. Kumar, **U. Kashyap**, S. S. Ali, *"De-Fake: Style-Based Anomaly Deepfake Detection."* preprint arXiv:2507.03334, 2025.
5. S. M. Shahid, S. K. Padhi, **U. Kashyap**, S. S. Ali, *"Generalized Deepfake Attribution."* preprint arXiv:2406.18278, 2024.

FELLOWSHIPS & AWARDS

- **TIH PhD Fellowship:** Awarded by the Technology Innovation Hub (TIH) for research on AI-driven GST fraud detection (Dec 2023 – May 2025).
- **National Eligibility Test (UGC-NET):** Qualified **6 times** (2019–2025), demonstrating consistent top-tier academic competency nationwide.
- **NFOBC Doctoral Fellowship:** Awarded by University Grants Commission (2023, 2024).
- **CG-SET Qualified:** Chhattisgarh State Eligibility Test (2019).

RESEARCH & PROFESSIONAL EXPERIENCE

PhD Research Scholar *Jan 2022 - Present*
MIST Lab, IIT Bhilai

- Led the development of a security benchmark for perceptual encryption, identifying critical vulnerabilities in existing state-of-the-art methods.
- Designed "De-Fake," a novel style-based anomaly detection framework for identifying deepfakes, improving detection rates on unseen datasets.

- Conducted extensive adversarial evaluation on malware detection systems, proposing robust countermeasures against evasion attacks.

Project Scientist *Jan 2023 - Dec 2023*
Indian Institute of Technology (IIT) Delhi

- Collaborated on the evaluation of next-generation wireless communication systems using ML-driven optimization techniques.
- Validated performance metrics through rigorous experimental setups and produced technical documentation for grant compliance.

Guest Faculty (Computer Science) *2020 - 2022*
Atal Bihari Vajpayee University

- Taught core curriculum: Machine Learning, Data Structures, and Programming.
- Mentored undergraduate students on capstone projects focusing on applied ML.

TECHNICAL SKILLS

Languages	Python, C, C++, LaTeX, SQL
ML Framework	PyTorch, TensorFlow, Keras, Scikit-learn, Numpy, Pandas, Seaborn, Matplotlib, Open-CV
Tools & Platforms	Git, Docker, Linux, Google Colab, Jupyter, Hugging Face
Core Competencies	Model Robustness, Adversarial Attack/Defense, Computer Vision, NLP

LANGUAGES

Hindi: Native **English:** Professional