

Ravi Prakash Srivastava

(+91)9431334691
raviprakashshrivastav7@gmail.com
er-ravi-srivastava.github.io
linkedin.com/in/ravi-prakash-sri

Summary

Software Engineer and AI Researcher with a Master's degree in Data Science & AI, specializing in Trustworthy AI, LLM Security, and Adversarial Machine Learning. Actively seeking PhD opportunities to advance research in secure, robust, and reliable AI systems.

Researcher Unique Identifiers

Google Scholar scholar.google.com/citations?user=sEIDRIMAAAAJ
ORCID orcid.org/0009-0009-3255-8758

Education

2024–2026 **M.Tech. in Data Science & Artificial Intelligence**.
Indian Institute of Information Technology, Ranchi, India — CGPA: 8.79/10

2018–2022 **B.Tech. in Information Technology**.
North-Eastern Hill University, Shillong, India — CGPA: 7.85/10

Professional Experience

Mar 2026 – Present **Software Engineer**, *SS Software Solutions LLC*, Hyderabad, India.

- Designed and standardized ML pipeline infrastructure: model versioning (**MLflow**, **DVC**), JSON-schema structured logging, observability monitoring and drift detection. Improved reliability across production models and cut incident diagnosis time by about **40%**.
- Built security and governance into ML workflows with **STRIDE** threat modeling, SAST (**Bandit**, **Semgrep**) and dependency vulnerability scanning in **GitHub Actions** CI/CD, reducing security-review effort and improving deployment reliability.

Aug 2022 – Feb 2023 **Machine Learning Intern**, *Centre for Development of Advanced Computing (C-DAC), Government of India*, Hyderabad, India.

- Developed machine-learning models that predict student academic performance from educational data.
- Implemented and benchmarked Decision Tree, Random Forest and Support Vector Machine models for the prediction task.

Research Projects

2026 **Cross-Domain Text Summarization Using Transformer Models**, *M.Tech. thesis*.

- Studied domain shift and catastrophic forgetting when adapting **BART-large-CNN** from news summarization to legal documents (**BillSum** dataset).
- Combined parameter-efficient fine-tuning (**LoRA**) with **Elastic Weight Consolidation (EWC)** to preserve pre-trained knowledge during domain adaptation.
- Improved cross-domain generalization while training only ~2M of the model's 406M parameters (under 1%), sharply reducing GPU memory use and training cost.

Awards & Honors

2026 **Best Paper Award**, ICACA 2026, for "Adversarial Prompt Injection Attacks on Large Language Models: Cryptographic Key Leakage and Defense Strategies."

2024–2026 **IETE Scholarship** for academic excellence throughout the 2 Year Master's program.

Publications

Journal Articles

2025 **Ravi Prakash Srivastava**, Sanjay Dahiya, and Aashish Nehra. IoT-HITS: An IoT Based Human Intrusion DeTection System for Border Region Using Deep Learning. *IETE Journal of Research*, 71(11). Taylor & Francis, July 2025.

2022 Ajay Kumar, Mohammad Amir Khusru Akhtar, Abhishek Pandey, and **Ravi Prakash Srivastava**. Smart City Vehicle Accident Monitoring and Detection System Using (MEMS, GSM, GPS) Raspberry Pi 4. *IETE Journal of Research*, 69(11):8121–8129. Taylor & Francis, March 2022.

Refereed Conference Papers

2026 **Ravi Prakash Srivastava**, Sourabh Sah, Kirti Kumari, Pavan Vovveti, and Md. Shah Fahad. Adversarial Prompt Injection Attacks on Large Language Models: Cryptographic Key Leakage and Defense Strategies. In *Proceedings of the International Conference on Advances in Computing and Applications (ICACA 2026)*, Lecture Notes in Networks and Systems, Ranchi, India, March 2026. Springer Nature. In press. **Best Paper Award**.

2026 Sourabh Sah, **Ravi Prakash Srivastava**, Kirti Kumari, and Md. Shah Fahad. Deepfake Video Detection Using Face-Centric Processing and Frame Sampling. In *Proceedings of the International Conference on Advances in Computing and Applications (ICACA 2026)*, Lecture Notes in Networks and Systems, Ranchi, India, March 2026. Springer Nature. In press.

2026 Sairamakrishna BuchiReddy Karri, **Ravi Prakash Srivastava**, Kiran Kumar Kadimi Chenchu, Ravina Marilyn Banze, and Ryan Banze. AI-Powered Code Review Assistant: Eliminating LLM Pipeline Using AST-Enhanced Hallucination to Analyze Pull Requests Automatically. In *Proceedings of the International Conference on Network Security and Blockchain Technology (ICNSBT 2026)*, Lecture Notes in Networks and Systems, Kolkata, India, 2026. Springer Nature. Accepted.

Preprints

2025 Jasmaine Khale and **Ravi Prakash Srivastava**. Balanced Few-Shot Episodic Learning for Accurate Retinal Disease Diagnosis. arXiv preprint arXiv:2512.04967 [cs.CV], December 2025.

Professional Service & Memberships

2026 **Reviewer**, International Conference on Innovations in Computing, Communication, and Sustainable Technologies (ICICST 2026), Dr. B. R. Ambedkar National Institute of Technology Jalandhar, April 3–5, 2026.

Since 2022 **Associate Member (AMIETE)**, Institution of Electronics and Telecommunication Engineers (IETE), India.

Technical Skills

Programming	Python, C++, Java, JavaScript
LLMs & NLP	LLMs, Transformers, PEFT (LoRA), Continual Learning (EWC), Text Summarization
ML & DL	Deep Learning, Computer Vision, Deepfake Detection, Efficient AI, Classical ML
MLOps	MLflow,Docker, Git, GitHub Actions (CI/CD), Model Monitoring
ML Security	STRIDE Threat Modeling, SAST (Bandit, Semgrep), Dependency Scanning, LLM Security
Systems	Linux/Unix, High-Performance Computing (HPC)
Languages	English, Hindi