Dr. K Naveen Kumar

+971 50 149 7846 | naveen.kummari@mbzuai.ac.ae

LinkedIn | Google Scholar | Federated Learning Made Easy

Hyderabad, Telangana State - 502284, India

Research Interests

- Security for Privacy-Preserving Machine Learning (Federated Learning) with Adversarial and Defender Perspectives
- Developing Secure and Private Vision LLMs for Medical AI Applications
- Ensuring Trustworthy Federated Learning through Verifiability, Auditability, and Mitigability
- Enhancing Autonomous Vehicle Technology in Transitional Weather Conditions
- Traffic Congestion Forecasting and Estimation using Aerial Video Analysis

Academic Background

- **Mohamed bin Zayed University of Artificial Intelligence (MBZUAI)** *Apr 2025 - now*
  Postdoctoral Research Associate Masdar City, Abu Dhabi, UAE
  - **Department:** Machine Learning
  - **Supervisor:** Prof. Mohsen Guizani
- **Indian Institute of Technology Hyderabad (IIT Hyderabad)** *Jan 2020 - Dec 2024*
  Doctor of Philosophy (PhD) Hyderabad, India
  - **Department:** Computer Science & Engineering
  - **Thesis:** Navigating Adversarial Attacks and Defense Mechanisms in Federated Learning: A Dual Perspective Approach
  - **Supervisor:** Prof. C Krishna Mohan
  - **CGPA:** 9.38/10.00
- **Indian Institute of Technology Hyderabad (IIT Hyderabad)** *Jan 2019 - Dec 2019*
  Master of Technology (MTech) Hyderabad, India
  - **Department:** Computer Science & Engineering
  - **Thesis:** Defining Traffic States Using Spatio-Temporal Traffic Graphs on Aerial Videos
  - **Supervisor:** Prof. C Krishna Mohan
  - **CGPA:** 8.65/10.00
- **Indian Institute of Information Technology Vadodara (IIIT Vadodara)** *July 2014 - May 2018*
  Bachelor of Technology (BTech) Vadodara, India
  - **Department:** Computer Science & Engineering
  - **CGPA:** 8.97/10.00

Research Experience

- **Research Intern - Sahaj AI Software Pvt. Ltd.** *Oct 2023 - Mar 2024*
  Project title: *Optimized defense against poisoning attacks in federated learning for medical image classification* Bangalore, India
- **Visiting Research Scholar - University of Agder** *Jan 2023 - July 2023*
  Project title: *Optimized model poisoning attack in federated learning* Grimstad, Norway
  - **Host Supervisor:** Prof. Linga Reddy Cenkeramaddi, Professor, Department of Information and Communication Technology, University of Agder, Grimstad, Norway.
- **Visiting Research Scholar - Purdue University** *May 2022 - Sep 2022*
  Project title: *Mitigate the data poisoning attacks in federated learning using a precision-guided approach* USA
  - **Host Supervisor:** Dr. Aravind Machiry, Assistant Prof., Dept. of Electrical Engineering, Purdue University, USA.
- **Research Intern - TCS Research & Innovation Labs** *Jan 2022 - Dec 2022*
  Project title: *A non-convex optimization approach to mitigate data poisoning attacks in federated learning* Hyderabad, India
- **Visiting Research Scholar (online mode) - Hiroshima University** *Aug 2021 - Nov 2021*
  Project title: *Zero-shot 2D object detection in Autonomous Vehicles* Japan
  - **Host Supervisor:** Prof. Kurita Takio, Graduate School of Advanced Science and Engineering, Hiroshima University, Japan. Selected as part of the **International Linkage Degree Program (ILDP)**.

PUBLICATIONS: JOURNALS

J=JOURNAL

[J.1: IEEE T-IFS] **K. Naveen Kumar**, C. Krishna Mohan and Linga Reddy Cenkeramaddi, **Federated Learning Minimal Model Replacement Attack Using Optimal Transport: An Attacker Perspective**. *IEEE Transactions on Information Forensics and Security*, Vol. 20, pp. 478-487, **2025. [IF: 6.3]**

[J.2: Elsevier AIM] **K. Naveen Kumar**, C. Krishna Mohan, Linga Reddy C, and Navchetan Awasthi, **Minimal Data Poisoning Attack in Federated Learning for Medical Image Classification: An Attacker Perspective**. *Artificial Intelligence in Medicine (Elsevier)*, Vol. 159, **2024. [IF: 6.1]**

[J.3: IEEE T-PAMI] **K. Naveen Kumar**, C. Krishna Mohan, Linga Reddy C, **The Impact of Adversarial Attacks on Federated Learning: A Survey**. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, Vol. 46, Issue 5, pp. 2672-2691, **2024. [IF: 20.8]**

[J.4: Elsevier PR] **K. Naveen Kumar**, Debaditya Roy, Thakur Ashutosh Suman, Chalavadi Vishnu, and C. Krishna Mohan, **TSANet: Forecasting Traffic Congestion Patterns from Aerial Videos using Graphs and Transformers**. *Pattern Recognition (Elsevier)*, Vol. 155, pp. 110721, **2024. [IF: 8.0]**

[J.5: IEEE T-ITS] Kondapally Madhavi, **K. Naveen Kumar**, C. Krishna Mohan. **Towards a Transitional Weather Scene Recognition Approach for Autonomous Vehicles**. *IEEE Transactions on Intelligent Transportation Systems*, Vol. 25, Issue 6, pp. 5201-5210, **2024. [IF: 8.5]**

[J.6: Springer ICT] Chalamala Srinivasa R., **K. Naveen Kumar**, Singh Ajeet, Saibewar Aditya, and C Krishna Mohan, **Federated learning to comply with data protection regulations**. *CSI Transactions on ICT (Springer Nature)*, Vol. 10, Issue 1, pp. 47-60, **2022.**

PUBLICATIONS: CONFERENCES

C=CONFERENCE

[C.1: CVPR] **K. Naveen Kumar**, Ranjeet Ranjan Jha, C Krishna Mohan, and Ravindra Babu Tallamraju, **Fortifying Federated Learning Towards Trustworthiness via Auditable Data Valuation and Verifiable Client Contribution**. **Accepted** In *IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*, June, USA, **Feb 2025. [Rank: A*]**

[C.2: CVPR] **K. Naveen Kumar**, Reshmi Mitra, and C. Krishna Mohan, **Revamping Federated Learning Security from a Defender's Perspective: A Unified Defense with Homomorphic Encrypted Data Space**. In *IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*, pp. 24387-24397. IEEE. June, USA, **2024. [Rank: A*]**

[C.3: CODASPY] **K. Naveen Kumar,** Aravind Machiry, and C. Krishna Mohan, **Precision Guided Approach to Mitigate Data Poisoning Attacks in Federated Learning**. In *ACM Conference on Data and Application Security and Privacy (CODASPY)*, pp. 233-244. ACM. June, Portugal **2024**.

[C.4: IJCNN] Kondapally Madhavi, **K. Naveen Kumar**, C. Krishna Mohan, **Object Detection in Transitional Weather Conditions for Autonomous Vehicles**. In *International Joint Conference on Neural Networks (IJCNN)*, pp. 1-8. IEEE. June, Yokohama, Japan **2024**.

[C.5: ITSC] Debaditya Roy, **K. Naveen Kumar**, C. Krishna Mohan, **Defining Traffic States using Spatio-Temporal Traffic Graphs**. In *IEEE 23rd International Conference on Intelligent Transport Systems (ITSC)*, pp. 1-6, Rhodes, Greece **2020**.

[C.6: CCEM] **K. Naveen Kumar**, Reshmi Mitra, **Resource Allocation for Heterogeneous Cloud Computing Using Weighted Fair-Share Queues**. In *IEEE International Conf. on Cloud Computing in Emerging Markets (CCEM)*, pp. 31-38. IEEE, Bangalore, India **2018**. [Received Best Paper Award]

PUBLICATIONS: WORKSHOPS

W=WORKSHOP

[W.1: IMUS2024] K. Madhavi, **K. Naveen Kumar**, and C. Krishna Mohan, **TransWardX: An Explainable Black-box Object Detection Attack for Autonomous Driving in Transitional Weather Conditions**. In *First Workshop on Intelligent Mobility in Unstructured Environments*, . IEEE, Kolkata, India **2024**.

[W.2: COMSNETS] **K. Naveen Kumar**, Digvijay S Pawar, C Krishna Mohan, **Open-air Off-street Vehicle Parking Management System using Deep Neural Networks: A Case Study**. In *14th International Conference on COMmunication Systems & NETworkS workshop*, pp. 800-805. IEEE, Bangalore, India **2022**.

[W.3: AIPR] **K. Naveen Kumar**, C. Vishnu, R. Mitra and C. Krishna Mohan, **Black-box Adversarial Attacks in Autonomous Vehicle Technology**. In *IEEE Applied Imagery Pattern Recognition Workshop*, pp. 1-7, 2020 IEEE, Bangalore, India **2020**.

Patents

[Filed] Kondapally Madhavi, **K Naveen Kumar**, C Krishna Mohan, and Sobhan Babu, **System And Method For Performing Adaptive Object Detection In An Autonomous Vehicle System**, *Indian Patent Office*, Official journal No. 16219-274, **Application no. 202541001505**, Jan, 07, **2025**.

[Filed] Kondapally Madhavi, **K Naveen Kumar**, C Krishna Mohan, and Sobhan Babu, **System and Method for Generating Weather Transition Data for Autonomous Vehicle Training**, *Indian Patent Office*, Official journal No. 16219-273, **Application no. 202541000718**, Jan, 03, **2025**.

[Filed] Ajeet Kumar Singh, Srinivas Rao Chalamala, and **K Naveen Kumar**, **Method and System for Preventing Poisoning Attacks in Collaborative Learning Systems**, *Indian Patent Office*, **Application no. 202321039349,** June, 08, **2023**.

Funded Projects

- **Medicine from the sky** *Sep 2021 - Dec 2021*
  Project title: *Design and Development of AI-based real-time light-weight system medical drone delivery*
  - **Funded by:** Bold and Unique Ideas Leading to Development (BUILD), IITH
  - **Amount:** INR 100000 for 4 months
  - **Role:** Principal Investigator (PI), Project Lead
- **iV4V (Intelligent Voice for Vision)** *Aug 2020 – Jan 2021*
  Project title: *An intelligent and reliable audio assistance for visual impairment using AI*
  - **Funded by:** Bold and Unique Ideas Leading to Development (BUILD), IITH
  - **Amount:** INR 100000 for 6 months
  - **Role:** Principal Investigator (PI), Project Lead
- **M2Smart - Multimodal Regional Transport System** *May 2017-April 2022*
  Project title: *Smart Cities for Emerging Countries Based on Sensing, Network, and Big Data Analysis*
  - **Funded by:** JICA/ JST SATREPS, Japan
  - **Role:** Team Leader

Technical Skills

- Machine learning, deep learning, federated learning, supervised & unsupervised learning, and computer vision
- **Programming & Libraries:** Python, TensorFlow, PyTorch, and OpenCV

Academic Achievements & Awards

- **PhD Research Excellence Award - Department of CSE** *2023-2024*
  Indian Institute of Technology, Hyderabad
- **Research week with Google** *2022-2023*
  Google
- **Top 10 finalist in Nvidia AI Hackathon** *2019*
  C-DAC Pune, Maharashtra, India
- **Selected for IITH-RU Project-Based learning program** *2019*
  Ritsumeikan University , Japan
- **Best Research Paper Award IEEE CCEM 2018** *2018*
  Bangalore, India

Invited Talks/ Guest of Honor

- **[Guest of Honor] Int. Conference on Intelligent Systems and Computational Networks (ICISCN 2025)** *January 2025*
  Lingraj Appa Engineering College, Bidar, Karnataka, India
  - Delivered a Keynote on Building Trust in Artificial Intelligent Systems: Innovations in Data Privacy and Security
- **International Conference On Distributed Systems, Computer Networks, and Cybersecurity (ICDSCNC)** *September 2024*
  Sri Krishna Institute of Technology, Bangalore, Karnataka, India
  - Pre-conference workshop on AI ML for Multi-domain Applications
- **Faculty Development Program (FDP)** *June 2024*
  Khaja Bandanawaz University, Karnataka, India
  - FDP on Artificial Intelligence and Data Science: Insights, Practices, and Applications
- **3rd International Conference On Distributed Computing and Electrical Circuits and Electronics (ICDCECE)** *April 2024*
  Ballari Institute of Technology and Management, Ballari, Karnataka, India
- **3rd International Research Workshop on Advances in Deep Learning and Applications (WADLA)** *December 2023*
  Indian Institute of Information Technology SriCity, India
- **IEEE International Conference on Integrated Intelligence and Communication Systems (ICIICS)** *November 2023*
  Sharnbasva University, Kalaburagi, Karnataka, India

Additional Information

- **Teaching Skills**
  1. Online two months AIML course for industry professionals **(June - Aug 2024)**
  2. **Teaching Assistant** for the below courses offered by Prof. C Krishna Mohan (PhD supervisor) at IIT Hyderabad
     - CS6450 - Visual Computing
     - CS6140 - Video Content Analysis
     - CS6170 - Computer Vision for Autonomous Vehicle Technology
     - CS6870 - Surveillance Video Analytics
- **Workshops/Technical Events**
  1. **Organized:** INCAPS 2022 at IIT Hyderabad Oct 2022
  2. **Attended: The Foundation for Academic Excellence and Access (FAEA Workshop)** in New Delhi from Dec 2017 to Jan 2018
- **Scholarships**

  Scholar (CC-20153914) Foundation for Academic Excellence and Access (FAEA), India Selected as one among 50 merit students all over India in the batch of 2015 and received a scholarship for three years.
- **External Reviewer**
  - IEEE Security and Privacy (2022, 2023)
  - IEEE Transactions on Information Forensics and Security (2023)
  - Elsevier Neurocomputing (2023)