Special Track Proposal Format

2nd International Conference on Advances in Artificial Intelligence for Society (ICA2S-2026)

Organized by **Indian Institute of Information Technology Bhopal, India**
In collaboration with **University of Vizja, Warsaw, Poland**

1. Title of the Special Track

Federated Learning and Privacy-Preserving AI for Secure and Scalable Intelligent Systems

2. Track Description

With the rapid expansion of data-driven technologies, Artificial Intelligence (AI) has become a cornerstone of modern intelligent systems across domains such as smart cities, finance, autonomous systems, industrial IoT, and social platforms. However, the growing reliance on large-scale data raises significant concerns regarding privacy, data security, and regulatory compliance. Traditional centralized learning paradigms often require aggregating sensitive data, leading to increased risks of data leakage and limited collaboration across distributed environments.

Federated Learning (FL) has emerged as a transformative paradigm that enables decentralized model training while preserving data privacy by keeping data localized at source devices. When combined with advanced privacy-preserving techniques such as differential privacy, homomorphic encryption, and secure multi-party computation, FL provides a robust foundation for building secure and trustworthy AI systems.

This special track aims to bring together cutting-edge research on federated and privacy-preserving AI across diverse application domains. It emphasizes scalable, communication-efficient, and robust learning frameworks, as well as solutions addressing challenges such as data heterogeneity, adversarial threats, model fairness, and explainability. The track seeks to foster interdisciplinary collaboration and promote innovative approaches that enable secure, distributed intelligence in real-world environments.

4. Topics of Interest

Topics include but are not limited to:

1. Federated Learning Algorithms and Architectures
2. Privacy-Preserving Machine Learning and Deep Learning
3. Differential Privacy and Data Anonymization Techniques
4. Homomorphic Encryption and Secure Computation
5. Secure Multi-Party Computation in Distributed AI
6. Federated Learning in IoT, Edge, and Cloud Systems
7. Communication-Efficient and Scalable FL Methods
8. Robust and Adversarially Secure Federated Models

9. Cross-Domain and Cross-Silo Federated Learning
10. Trustworthy, Fair, and Explainable AI
11. Blockchain for Secure and Decentralized AI Systems
12. Privacy, Ethics, and Governance in AI Systems

5. Special Track Organizers

Name: Faheem Ahmad Reegu
Designation: Assistant Professor
Department: College of Engineering and computer Science , Department of Electrical and Electronics Engineering
Institution: Jazan University , Saudi Arabia
Country: Saudi Arabia
Email: freegu@jazanu.edu.sa
ORCID (optional): https://orcid.org/0000-0002-9167-3061

Co-Organizer (if any):
Name: Dr Ihtiram Raza Khan
Designation: Professor
Department: Computer Science Department
Institution: Jamia Hamdard Delhi
Country: India
Email: erkhan2007@gmail.com
ORCID (optional): 0000-0001-9196-4451

6. Contact Information

Primary Contact Person: **: Faheem Ahmad Reegu**
Email: freegu@jazanu.edu.sa
Phone (optional):