1. Title of the Special Session: **Recent Trends of Security in Data Science and Machine Learning**

2. Objective of the Session

   The main objective of this session is to impart an opportunity to Scholars, researchers, academicians, and industry professionals from varied background areas to exchange the latest research ideas and research and development on Machine Learning, emerging security technologies on machine learning, and Data Science. Both the technologies (Data science and machine learning) are providing exponential rise in the field of innovation and hence becoming more popular day by day.

   **Rationale**: Despite their immense popularity security in them is a big concern. The concept of new security mechanisms in data science and machine learning allows making use of the computing process more actionable and intelligent as compared to traditional methods. This Special Session will deal with the recent trends in the security field for varied applications of Machine learning, Data Science in relevance to various aspects of our real life.

3. Topics of the Session

   We are inviting high-quality research for submission in the Special Session based on the above-mentioned theme including the following topics but not limited to

   - Security aspects in Data Science Parallel and Distributed Computing.
   - Privacy in Data Science for Autonomous Vehicles.
   - Security Loopholes Big Data Analysis and Applications.
   - Secure Business Intelligence and Data Analytics.
   - Data Science for Detecting, Preventing, and Predicting Web Data Anomalies.
   - Security Mechanisms for Statistical Learning for Data Science.
   - Improved Secure Data Mining
   - Traditional Security measures for pattern recognition
   - Various aspects of security in Social Networks Analysis.
   - Secured Intelligent Agents and Systems.
   - Improved secured various Evolutionary, Meta Heuristics, Nature Inspired, Algorithms
   - Malicious Language Processing framework
   - Securing machine learning systems
   - Artificial intelligence in Healthcare
   - Transfer learning attacks, vulnerabilities, and countermeasures in ML

4. Proposer full name and affiliation (names, designation, affiliation and contact emails)

   Dr. Dimple Nagpal , Dr. Sumit Badotra