

Special Session on Security and Trust in Computational Intelligence

CALL FOR PAPERS:

Today the networks around the world are computing humongous data. The leveraging technologies capturing data continuously from IoT Networks, Edge Networks, and processing on-demand over the cloud has enabled applications across the service industry and manufacturing units. The Big Data so collected provides an opportunity to extract meaningful insights and automate the computational process and elevate the service instruments and structure the decision-making process for businesses. Precisely speaking, the Big Data has provided a base to implement and devise Computational Intelligence models, algorithms, and computational methods inspired by Biology, Nature, and Swarm Intelligence for experimental and experiential learning. The AI-based models, methods, and framework devised for scalable and distributed Big Data over the cloud. However, the security of the Big Data so generated is an open problem. Extracting useful insights in real-time has an equivalent threat to the computing services. Even today the entire computational architecture is vulnerable to data leakage and privacy issues. The trust management issues are prevailing across distributed systems, and edge networks, and therefore there is an insatiable need to align the model, method, and process for Real-Time Big Data for Computational Intelligence to penetrate the evolving business Insights. There is a need to investigate the privacy, security, and trust issues in Computational Intelligence and identify advanced solutions for Computational Intelligence. The Special Session aims to provide the novel and the latest research and discussion forum from research scholars, academicians, and industry practitioners. The Special Session invites authors from broad disciplines and backgrounds like Computational Intelligence, Expert Systems, Explainable AI IoT, Edge Computing, Distributed Cloud Computing, Big Data Analytics, Cyber Security, Data Privacy, Trust Management, Bio-Inspired, Nature Inspired and, Swarm Inspired Intelligence to present original and latest advancements with respect to data privacy, security and trust management.

The special session will include the following broad topics,

- Issues, opportunities, and challenges faced by IoT Networks
- Assessing Data Privacy, Security, and Trust in Cloud and Edge Networks
- Original and Novel Theories for modeling data privacy, security
- Advances in data privacy, security, and trust in Computational Intelligence/ Frameworks for Privacy, Security, and Trust Management in Computational Intelligence
- Bio-inspired, Nature Inspired, and Ant Colony Optimization (ACO) based Algorithms for Computational Intelligence
- Swarm Intelligence Inspired Algorithms for Computational Intelligence
- Reinforcement Learning Models for Data Privacy, Security, and Real-Time Trust Management
- Advances in Fairness and Recommendation based Computational Intelligence
- Preserving Privacy, Security, and Trust in Big Data
- Preserving Privacy, Security, and Trust in Explainable, Understandable, and Responsive AI, Federated ML, Deep Learning
- Assessing Data Privacy, Security, and Trust in E-Commerce
- Privacy Preserving in Blockchain for Computational Intelligence
- Advances in Encryption for Computational Intelligence
- Use cases, Case Studies, and Applications for Security and Trust based on Computational Intelligence

Special Session Chair

Prof. (Dr.) B. Balamurugan Balusamy, Galgotias University, U.P, India
Prof. (Dr.) Vandana Sharma, Galgotias University, U.P, India