ICICC-2023
6th International Conference on Innovative Computing and Communication

Organized by ShaheedSukhdev College of Business Studies, New Delhi, India
On 17-18th FEBRUARY 2023.

********** CALL FOR PAPERS **********

SPECIAL SESSION ON
Security and Privacy in the Cloud

SESSION ORGANIZERS

Prof. Naren.J, Assistant Professor, School of CS and IT, JAIN (Deemed-to-be University), Bangalore.
Dr. Suchitra. R. Nair, Professor and Head, School of CS and IT., JAIN (Deemed-to-be University), Bangalore.

SESSION DESCRIPTION:

Security and Privacy has been a buzzword in the field of Cloud Compuitng in general. The Special Session on Security and Privacy in the Cloud using Machine Learning Applications will act as a major forum for the presentation of innovative ideas, approaches, developments, and research projects in the areas of Cloud computing, Security and Machine Learning. It will also serve to facilitate the exchange of information between researchers and industry professionals to discuss the latest issues and advancement in the area of Cloud Computing, Security and Machine Learning Recent advances in computing and information technologies such as IoT, mobile Edge/Cloud computing, cyber-physical-social systems, Artificial Intelligence/Machine Learning/ Deep Learning, etc., have paved way for creating next generation smart and intelligent systems and applications that can have transformative impact in our society while accelerating rapid scientific discoveries and innovations. Such newer technologies and paradigms are getting increasingly embedded in the computing platforms and networked information systems/infrastructures that form the digital foundation for our personal, organizational and social processes and activities. It is increasingly becoming critical that the trust, privacy and security issues in such digital environments are holistically addressed to ensure the safety and well-being of individuals as well as our society.

RECOMMENDED TOPICS:
Topics to be discussed in this special session include (but are not limited to) the following:

- Foundational, theoretical models for trust, privacy and security in emerging applications
- Trusted AI, Machine Learning and Deep Learning
- Privacy preserving Machine Learning and Deep Learning
- Trustworthy, safe and resilient intelligent systems
- Trusted, privacy-conscious and secure systems, applications and networks/infrastructures
- Security and privacy in IoT and Cyber-physical-human systems
- Trustworthy and secure Human-Machine collaboration
- Access and trust management/negotiation, and secure information flow/sharing
- Bio-inspired approaches to trust, privacy and security
- Game theoretical approaches to trust, privacy, and security
- Adversarial machine learning
- Trust, privacy and security for big data systems, applications and platforms
- Trust, privacy and security for smart cities and urban computing
- Machine Learning / Deep learning over encrypted data
- Usability and human factors for trust, privacy and security
- Tools, techniques and metrics for trust, privacy and security
- Anonymization techniques and differential privacy for emerging intelligent applications
- Trust, privacy and security approaches for services computing: microservices, service-oriented architectures, service composition and orchestration
- Blockchain and Distributed-ledger technologies
- Blockchain/Distributed ledger for e-commerce, mobile commerce and intelligent applications
- Bias, fairness and integrity/robustness of algorithmic machine / AI algorithms
- Trusted, privacy-aware and secure interoperation of interacting/collaborative systems
- Threat models and attack modeling for AI/ML and applications
- Identification/Detection of spam, phishing, malware and APTs
- Cryptographic approaches and secure multiparty computation
- Privacy-preserving data mining and big data analytics
- Application of AI/ML and Deep learning for trust, privacy and security
- Trust, privacy and security in edge/cloud computing, social computing
- Safe and trusted autonomous vehicles/UAVs, robotics
- Trust, security and safety in supply-chain environments and critical infrastructures
- Data quality/credence, privacy and provenance
- Trust in social media – disinformation/misinformation
- Risk metrics and measurements, assessment/analysis and mitigation
- Insider threat modeling, analysis and mitigation; behavioral modeling for security and trust
- Digital payments and cryptocurrencies; Secure and trustworthy e-commerce and mobile commerce
- Trust negotiation and/or propagation in interacting systems of systems, multi-agent systems, and social networks.

SUBMISSION PROCEDURE:

Researchers and practitioners are invited to submit papers for this special theme session on **[Security and Privacy in the cloud]** ***on or before*** **[10th December 2022]**. All submissions must be original and may not be under review by another publication. INTERESTED AUTHORS SHOULD CONSULT THE CONFERENCE'S GUIDELINES FOR MANUSCRIPT SUBMISSIONS at

http://icicc-conf.com/paper_submission.html. All submitted papers will be reviewed on a double-blind, peer review basis.

NOTE: While submitting paper in this special session, please specify [**Security and Privacy in the cloud with Machine Learning Applications**] at the top (above paper title) of the first page of your paper.

* * * * * *