Message from the Editor-in-Chief

Computing and communication technologies are at the heart of societal advancements in transportation, production and manufacturing, logistics, healthcare, utility, recreation, social, and many other domains. While these advancements offer profound benefits, they also pose new security and privacy challenges that can undermine these advancements. It is possible now for adversaries to exist anywhere and at any time in the data life cycle. Adversaries might attempt traditional attacks intended to subvert the confidentiality, integrity, and availability of these new cyber systems and, while such threats can lead to privacy, data, and economic damage, they can also lead to physical damage to the world around us and directly affect our personal well-being. New developments in the science and engineering of cybersecurity are needed in order to provide the tools that are necessary to protect our society and the investments we have made across a variety of domains. Further, collaboration between technology, policy, legality, and economics is needed in order to arrive at the best solutions to mitigate the emergence and impact of cybersecurity threats before they occur.

Author Benefits

- **Open Access** Unlimited and free access for readers
- **No Copyright Constraints** Retain copyright of your work and free use of your article
- **Thorough Rigorous Peer-Review**
- **No Space Constraints, No Extra Space or Color Charges** No restriction on the length of the papers, number of figures or colors
Aims and Scope

*Journal of Cybersecurity and Privacy* (ISSN 2624-800X) is an online, open access, peer-reviewed journal which provides a forum for the dissemination of research related to all technical areas of cybersecurity.

The main topics of *Journal of Cybersecurity and Privacy*:

- Anomaly and intrusion detection, and countermeasures to prevent detection
- Applied cryptography and cryptographic protocols
- Authentication and identity management technologies
- Big data security and privacy
- Cloud computing and security and privacy threats in the cloud
- Forensics, including computer and network forensics
- Information-theoretic security and network security
- Legal and public policy aspects of security and privacy
- Malware, malware reverse engineering, and malware defense and mitigation strategies
- Physical layer security and cross-layer security for communications
- Privacy and privacy enhancing technologies, including applications to new domains
- Security metrics and the science of security