



## Challenges and Remedies of IR4 Network Security

Guest Editors:

**Prof. Dr. Sundararaja  
Sitharama Iyengar**

Knight Foundation School of  
Computing and Information  
Sciences, Florida International  
University, Miami, FL, USA

**Dr. K. J. Latesh Kumar**

Knight Foundation School of  
Computing and Information  
Sciences, Florida International  
University, Miami, FL, USA

Deadline for manuscript  
submissions:

**closed (30 June 2023)**

### Message from the Guest Editors

Security is never-ending, and the rule regarding its implementation is considered to be “trust no one”. The age of artificial intelligence is a pathway paved with the aim of isolating legacy threat detection with the new “prediction” technique. Henceforth, let us ponder the innovation of next-generation strong network systems that can discover threats in advance, with the aim of protecting the world’s security. Topics include, but are not limited to, the following:

1. AI-powered network spike detection: learning models that can sense network threats in advance;
2. Reinforced network security: machine-learned self-constructing network systems;
3. Next-generation sense systems: learn, predict and act out characteristics and behavior of network threats;
4. Case studies on network traffic-based threat effectiveness and countermeasures using AI/ML techniques;
5. Network tampering and tamper resistance;
6. Creating AI-based network systems to pathway the quantum network;
7. Reverse engineering and countermeasures for network threats;
8. Creating secured network integrations with higher level software, firmware and microarchitectures.

Welcome to contribute!

