

Chip to Cloud security: Trends and Challenges

Session Chair: Dr. Shubhalaxmi Kher, Arkansas State University, USA

In the context of cloud computing paradigm, security of existing systems needs to be revisited. Cloud security is a very challenging issue mainly due to the diversity of networks in the cloud that are vulnerable to attacks. To address this issue, the approach needs to consider the distributed nature of the cloud. Towards secured cloud, research efforts are mainly to provide software solutions though limited hardware security efforts like Samsung Galaxy SIII exists. In an open and ubiquitous distributed environment, where data access is required by anyone spontaneously, strong authentication mechanisms are required. In this context, for authentication, traditional access control approaches based on identity, where it is assumed that the users are known to the provider through a process of registration may not be sufficient. This session will bring in focus on hardware security embedded on the chip and software solutions to cyber threats. The papers in this session will include; but not limited to:

- Cloud Services Security and other Enterprise-Level security.
- Authentication technologies
- Secure hardware technologies and PLC security testing
- Run-time & design time reconfigurable secure platforms & processors
- Self Organized networks for organizing versatile resources