IEEE International Conference on Communications

16-20 May 2022 // Seoul, Korea

Intelligent Connectivity for Smart World

Workshop on Blockchain for Secure Software-defined Networking in Smart Communities (BlockSecSDN)

General Co-chairs

- **Gagangeet Singh Aujla**
  Durham Univeristy, UK
- **Anish Jindal**
  University of Essex, UK
- **Neeraj Kumar**
  Thapar University, India
- **Harpreet Singh Dhilon**
  Virginia Tech, USA

Main contact

gagangeet.s.aujla@durham.ac.uk
anishjindal90@gmail.com

Important Dates

- ❖ Paper submission deadline: **January 20, 2022**
- ❖ Notification of acceptance: March 06, 2022
- ❖ Camera-ready papers: March 15, 2022

Submission link

https://edas.info/N28800

Webpage link

https://sites.google.com/view/iblocksecsdn2022

Scope

The emergence of SDN technology helps to isolate the control plane from the data plane and solves the issues through network programmability. The SDN is a centralized approach and easily modify the network topology, and besides, maintain data consistency and interoperability among heterogeneous IoT devices with the help of automation. Although SDN technology performs resilient and reliable connections in the heterogeneous environment based on secure communication protocols designed by the network programmers still chances of security threats may occur as a single controller is handling the complete network infrastructure. With the widespread adoption of wireless sensors in smart communities, device-to-device communication is susceptible to security vulnerabilities and resulting in devastating attacks on the network controller. Nowadays, Blockchain, a distributed ledger, is often linked to the financial service industry due to the concept of its underlying inception and the success, i.e, bitcoin. But, it is a wrong conception to confine blockchain to only one vertical. Contrary to popular opinion, blockchain can be closely associated with security and thereon can transverse across all the industries and smart communities. The distributed ledger shifts focus from a single and centralized point of failure towards a complex and intertwined decentralized model. Under this umbrella, one possibility is the blockchain for Secure SDN, and large scale network enterprises are already investing and exploring this opportunity.

Topics

We seek original completed and unpublished work not currently under review by anyother journal/magazine/conference. Topics of interest include, but are not limited to:

- Security and privacy for innovative service delivery models.
- Lightweight Cryptography in wireless sensors nodes for SDN security.
- Quantum Cryptography in heterogeneous IoT devices for SDN security.
- Blockchain for secure device-to-device communication in SDN.
- Authentication, authorization, and access control for SDN security.
- Blockchain for anomaly detection in smart communities.
- Blockchain for secure integration of IoT and fog devices for SDN.
- Intrusion detection and prevention system for SDN security.
- Heterogeneous blockchain models and trustworthy architectures.
- Blockchain for secure data storage and computing model in SDN.
- Testbed and experimental components tailored to specific BlockSecSDN.
- Blockchain for secure transaction management using SDN.
- Deduplication architectures for blockchain-enabled cloud storage.

Paper Submission

The workshop accepts only novel, previously unpublished papers. The page length limit for all initial submissions for review is SIX (6) printed pages (10-point font) and must be written in English.All final submissions of accepted papers must be written in English with a maximum paper lengthof six (6) printed pages (10-point font) including figures. No more than one (1) additional printed page (10-point font) may be included in final submissions and the extra page (the 7th page) will incur an over length page charge of USD100. For more information, please see IEEE ICC 2022 official website: https://icc2022.ieee-icc.org/authors