Association for Computing Machinery

ACM Transactions on Internet Technology– Special Issue on

Blockchain-based Zero Trust Cybersecurity in the Internet of Things

Special Issue Guest Editors

Dr. Shancang Li
(Corresponding GE)
University of the West of England, Bristol, UK
Shancang.li@ieee.org

Dr. Surya Nepal
CSIRO's Data61, Sydney, Australia
Surya.Nepal@data61.csiro.au

Dr. Theo Tryfonas
University of Bristol, Bristol, UK
Theo.Tryfonas@bristol.ac.uk

Prof. Hongwei Li
University of Electronic Science and Technology of China, Chengdu, China
Hongweili@uestc.edu.cn

Important Deadlines

- Manuscript submission: April 30, 2021
- First notification: June 30, 2021
- Submission of revised manuscript: Aug 31, 2021
- Final notification: Sep 30, 2021
- Final submission (camera-ready): October 30, 2021

ACM TOIT Editor-in-Chief

Prof. Ling Liu
School of Computer Science, Georgia Institute of Technology
ling.liu@cc.gatech.edu

The Internet of Things (IoT) connects a massive number of smart devices to the Internet, in which all data, applications, devices, and users require connectivity, security and trust. Traditional security approaches assume that all participants within the network perimeter are trustworthy. However, in IoT environment data, applications, devices, and users are gradually moving outside the traditional trusted defence perimeter and have become a source of security risks. Unlike traditional security approaches, which are initially designed for the optimum protection and only act if a process is malicious, the zero-trust security framework upholds "verify and never trust" principle. Zero trust-based approaches assume that everything within the system is untrustworthy and needs to be verified to prevent threats.

Meanwhile, the blockchain technology shows promises on cybersecurity and several blockchain security mechanisms have been developed, including access management, user authentication, and transaction security. Due to its prowess in enhancing cybersecurity, blockchain can provide zero trust security framework with highly accessible and transparent security mechanisms via a visible blockchain, in which all transactions are visible to restricted operators. Zero-trust models can be secured further by a blockchain due to its sheer immutable nature and blockchain technology is expected to recognise them, authenticate their trust and allow them access. Blockchain-enabled zero trust security can detect suspicious online transaction, isolate connection, and restrict access to the user.

This special issue aims to bring together researchers from both academia and industry to discuss the most recent advances on zero trust cybersecurity and blockchain in the IoT environment.

The topics of interest to this special issue include, but are not limited to:

- Zero trust architecture and security framework
- Zero trust networks and IoT systems
- Theories of zero trust and blockchain
- Strong authentication in zero trust
- Validate and verify the authentication of access in IoT
- Continuous monitoring and vulnerability assessment in IoT
- Blockchain and data security/privacy
- Blockchain-based trusted e-healthcare
- Blockchain-enabled authentication in IoT
- Applications of blockchain in IoT scenarios
- Lightweight cryptography in zero trust
- Anonymity in the blockchain and IoT
- Accountability and privacy in zero trust systems
- Implementation of zero trust in IoT
- 5G/6G enabled zero trust networks
- Zero trust security in smart cities
- Scalability of zero trust systems
- Artificial Intelligence/Machine Learning enabled zero trust
- Legal and regulatory issues in zero trust networks

Submission Instructions

For author guidelines, please refer to: this link.
E-mail alias for this special issue: blockchain-based@acm.org
EasyChair link for paper registration: click here
Paper submission will be through Manuscript Central. It will open one month before the submission deadline. Please select "Special Issue on Blockchain-based Zero Trust Cybersecurity in the Internet of Things" when submitting.