# Internet of Things Security: CyberAssurance for Edge, Software Defined, and Fog Computing Systems

Tyson Brooks
Syracuse University
ttbrooks@syr.edu

Shiu-Kai Chin
Syracuse University
skchin@syr.edu

## Abstract

*The objective of this mini-track is to increase the visibility of current research and emergent trends in Cyber-Assurance theory, application, embedded security and machine-learning for the Internet of Things (IoT), software-defined networks (SDN)/network function virtualization (NFV), Cyber-Physical Systems (CPS) and Fog computing architectures based on theoretical aspects and studies of practical applications. Cyber-assurance is the justified confidence that networked systems are adequately secure to meet operational needs, even in the presence of attacks, failures, accidents and unexpected events. Cyber-assurance means that IoT systems, smart internet connected devices (ICD) and networks provide the opportunity of automatically securing themselves against cyber-attacks. The difference is that the concept of cyber-assurance must provide embedded, secure microchips/processors in ICD devices and virtual networks that can continue to operate correctly even when subjected to an attack.*

## 1. Introduction

IoT devices and CPS using SDN/NFV and Fog computing systems and networks should be able to resist the various security cyber-attacks such as hacking of networks, devices, theft of information, disruption, etc. and be able to continue performing under severe environmental conditions. Through embedded processors and machine learning algorithms over the transmitted information, the miscoding and leaking of information during transmission channels has to monitor any loss, miscoding and leaking of data. Timely adjustments of information with falling quality and automatic switching to the best routing IoT systems by making uses of multi-directional routing is also warranted. Cyber-assurance will need to provide the principles and technologies to unify these systems to deliver the end-state goal of secure IoT systems for greatly enhanced interoperability, scalability, performance, and agility.

The target audience of this minitrack will be composed of researchers, professionals and students working in the field of cyber-security, wireless technologies, information system theory, systems engineering, information security architecture and security system design along with university professors and researchers involved in IA, IoT and Fog Computing related networking. Through the research identified for this track, graduate students, researchers and academics who want to improve contribute their understanding of the latest security developments for the IoT and Fog Computing. This minitrack will focus on the security needs of the IoT/Fog Computing environment, highlighting key issues and identifying the associated security implications so that the general participates can readily grasp the core ideas in this area of research.

The following articles will be included in this minitrack:

## 2. Minitrack Articles.

## MAHIVE: Modular Analysis Hierarchical Intrusion Detection System Visualization Event Cybersecurity Engine for Cyber-Physical Systems and Internet of Things Devices

*Abstract*:

Cyber-Physical Systems (CPS), including Industrial Control Systems (ICS) and Industrial Internet of Things (IIoT) networks, have become critical to our national infrastructure. The increased occurrence of cyber-attacks on these systems and the potential for catastrophic losses illustrates the critical need to ensure our CPS and ICS are properly monitored and secured with a multi-pronged approach of prevention, detection, deterrence, and recovery. Traditional Intrusion Detection Systems (IDS) and Intrusion Detection and Prevention Systems (IDPS) lack features that would

URI: https://hdl.handle.net/10125/71473
978-0-9981331-4-0

make them well-suited for CPS and ICS environments. We report on the initial results for MAHIVE: Modular Analysis Hierarchical IDS Visualization Event cybersecurity engine. MAHIVE differs from traditional IDS in that it was specifically designed and developed for CPS, ICS, a IIoT systems and networks. We describe the MAHIVE architecture, the design, and the results of our evaluation using two ICS testbed penetration testing experiments.

## A Systematic Mapping Study of Access Control in the Internet of Things

*Abstract:*

Internet of Things (IoT) provide wide range of services in both domestic and industrial environments. Access control plays a crucial role as to granting access rights to users and devices when an IoT device is connected to a network. Over the years, traditional access control models such as RBAC and ABAC have been extended to the IoT. Additionally, several other approaches have also been proposed for the IoT. This research performs a systematic mapping study of the research that has been conducted on the access control in the IoT. Based on the formulated search strategy, 1,617 articles were collected and screened for review. The systematic mapping study conducted in the paper answers three research questions regarding the access control in the IoT, i.e., what kind of access control related concerns have been raised in the IoT so far? what kind of solutions have been presented to improve access control in the IoT? what kind of research gaps have been identified in the access control research in the IoT? To the best of our knowledge, this is the first systematic mapping study performed on this topic