

---

## Editorial

---

### Tyson Brooks

School of Information Studies (iSchool),  
Syracuse University,  
343 Hinds Hall, Syracuse, NY 13210, USA  
Email: [ijitcaeditor@gmail.com](mailto:ijitcaeditor@gmail.com)

---

Welcome to the inaugural issue of the *International Journal of Internet of Things and Cyber-Assurance (IJITCA)*, which is published by Inderscience Publishers. We are excited to launch this venue and it's an honour to serve the *IJITCA*.

The internet of things (IoT) is the idea that virtually every physical 'thing' will one day be connected to the internet utilising embedded technology in these objects to allow internal and external interactions. These 'things' (e.g., smart internet-connected devices), whose identity can be transmitted to an internet-connected infrastructure, will be able to collect and broadcast data amongst these devices using various wired and wireless technologies.

The concept of cyber-assurance provides the justified confidence that networked systems are adequately secure to meet operational needs, even in the presence of attacks, failures, accidents and unexpected events. Security professionals have long recognised that 'embedded' protective mechanisms that are needed to counter cyber-threats must be built into these smart internet-connected devices and systems from their inception, rather than added on after the fact. This principle is especially relevant to the concept of cyber-assurance for the internet of things and the smart Internet-connected devices that will be used.

The *IJITCA* publishes papers on the latest advances, as well as review articles, on various aspects of IoT and cyber-assurance. Topics will include IoT security designs and architecture, IoT sensor networks and enabling technologies, IoT communications and networking protocols, and vulnerabilities in IoT devices and networks. Special issues will focus on single topic areas. Forthcoming examples include IoT based cloud computing, machine learning and the IoT, and securing IoT and fog computing architectures through cyber-assurance.

The need for the *IJITCA* in the research community provides an understanding of the cyber-assurance domain from an information security practitioner's perspective and the identification of major cyber-threats to the IoT. This inaugural issue publishes five articles addressing the secure deployment of IoT entities, bring your own device (BYOD) and IoT risks within an educational environment, an IoT survey of challenges and issues, a security analysis on Apple Pay and security and privacy issues with the Amazon Echo. I hope that the *IJITCA* will represent the IoT security community by becoming the international leader in IoT and cyber-assurance research.

I am truly honoured to launch the *IJITCA* as its Editor-in-Chief. This effort has become possible because of the diligent support of the *IJITCA* Editorial Board for their dedication and contributions. The Editorial Board of the *IJITCA* is composed of renowned experts in the fields of information security, IoT, system architecture and

analysis, security engineering and innovation throughout the world. Most *IJITCA* editorial board members hold distinguished university professorships and directorships of research centres at their respective institutions, have served or currently serving as presidents of professional organisations, and/or Editors-in-Chief and associate editors of globally recognised journals. I am totally confident that the *IJITCA* will make important contributions to the field and become a success under the guidance of such distinguished professionals.

The journal looks forward to receiving your submissions, suggestions, and volunteer services. Thank you all, in advance.