**Future Internet, MDPI** (covered by Emerging Sources Citation Index (ESCI-Web of Science), Ei Compendex, Scopus).
http://www.mdpi.com/journal/futureinternet

** **Special Issue on IoT Security and Privacy** **
http://www.mdpi.com/journal/futureinternet/special_issues/and_Privacy

As per recent estimates, the number of Internet of Things (IoT) devices will surpass 50 billion by 2020. Unsurprisingly, this mushrooming of IoT devices has drawn the attention of attackers who seek to exploit the merits of this new technology for their own benefit. The direct or indirect exposure of the limited resources IoT devices to the dangers of the Internet opens the door to a plethora of potential security and privacy risks to the end-users, including the unsanctioned access and abuse of private information, the enabling and strengthening of assaults against other systems, and the breeding of risks pertaining to personal safeness.
When considering conventional Internet applications, typical risks revolve around economic losses, leakage of personal private information and damage of reputation of the corporation. However, as IoT starts to penetrate to virtually all sectors of the society such as retail, transportation, home automation and even healthcare, any security breach may prove catastrophic to the actual user and its physical world. Such considerations may diminish the user's confidence towards the IoT technology as a whole and impede its adoption.
The special issue at hand intends to promote the dissemination of the latest methodologies, solutions, and case studies pertaining to IoT security and privacy issues. Its objective is to publish high-quality articles presenting security algorithms, protocols, policies, frameworks, and solutions for the IoT ecosystem. Only technical papers describing previously unpublished, original, state-of-the-art research, and not currently under review by a conference or journal will be considered.

**Possible topics of interest of this special issue include but are not limited to:**

- Security and privacy in heterogeneous IoT.
- Secure and Privacy Preserving Data Mining and Aggregation in IoT applications.
- Cross-domain trust management in smart networks.
- Secure authentication of IoT devices.
- MAC layer security protocols for the IoT applications.
- IoT security mechanisms targeting application layer protocols.
- Resource-savvy Intrusion Detection for Networks of Things.
- IoT-based malware mitigation.

**Deadline for manuscript submissions: 28 February, 2018**

**Guest Editors**

Dr. Georgios Kambourakis
Department of Information and Communication Systems Engineering
University of the Aegean, Samos, Greece
gkamb@aegean.gr
URL: http://www.icsd.aegean.gr/gkamb

Dr. Constantinos Kolias
Computer Science department
George Mason University, VA, USA
kkolias@gmu.edu
URL: https://mason.gmu.edu/~kkolias/