Security in Internet of Things: Issues, Challenges and Solutions

Guest Editor:

Prof. Dr. Rashid A. Saeed
Department of Computer Engineering, College of Computers and Information Technology, Taif University, P.O. Box 11099, Taif 21944, Saudi Arabia

Deadline for manuscript submissions:
closed (31 October 2023)

Message from the Guest Editor

Recently, Internet of Things (IoT) networks have been extensively addressed in the literature by scholars from both the industry and academia. IoT technology is expected to contribute to the global economy industry by more than USD 14 trillion by 2030, and is widely recognized as an integral part of the Fourth Industrial Revolution (4IR, or Industry 4.0). This great potential comes with many challenges and problematic issues, especially in terms of security. The purpose of this Special Issue is to identify threats that could challenge the privacy, integrity, authentication, confidentiality, denial of service (DoS), malware, data anomaly, eavesdropping and other potential vulnerabilities that authors may wish to study. Additionally, this Special Issue intends to propose new novel solutions for IoT vulnerabilities, i.e., cyber-physical techniques, blockchain, hardware security approaches, novel cryptographic techniques, etc. The SI will help the industry to identify major new security issues that may arise after deploying the IoT network and the potential solutions to these challenges.

Special Issue

Editor-in-Chief

Prof. Dr. Giulio Nicola Cerullo
Dipartimento di Fisica,
Politecnico di Milano, Piazza L.
da Vinci 32, 20133 Milano, Italy

Message from the Editor-in-Chief

As the world of science becomes ever more specialized, researchers may lose themselves in the deep forest of the ever increasing number of subfields being created. This open access journal Applied Sciences has been started to link these subfields, so researchers can cut through the forest and see the surrounding, or quite distant fields and subfields to help develop his/her own research even further with the aid of this multi-dimensional network.

Author Benefits

Open Access: free for readers, with article processing charges (APC) paid by authors or their institutions.
High Visibility: indexed within Scopus, SCIE (Web of Science), Inspec, CAPlus / SciFinder, and other databases.
Journal Rank: JCR - Q2 (*Engineering, Multidisciplinary*) / CiteScore - Q1 (*General Engineering*)

Contact Us