frontiers | Frontiers in Computer Science

TYPE Editorial
PUBLISHED 17 March 2023
DOI 10.3389/fcomp.2023.1173296

OPEN ACCESS

EDITED BY
Nicola Zannone,
Eindhoven University of Technology, Netherlands

REVIEWED BY
Savio Sciancalepore,
Eindhoven University of Technology, Netherlands

*CORRESPONDENCE
Antonino Rullo
✉ n.rullo@dimes.unical.it

SPECIALTY SECTION
This article was submitted to Computer Security, a section of the journal Frontiers in Computer Science

RECEIVED 24 February 2023
ACCEPTED 09 March 2023
PUBLISHED 17 March 2023

CITATION
Rullo A, Ianni M and Serra E (2023) Editorial: Security and privacy for the Internet of Things. *Front. Comput. Sci.* 5:1173296. doi: 10.3389/fcomp.2023.1173296

Editorial: Security and privacy for the Internet of Things

Antonino Rullo[1]*, Michele Ianni[1] and Edoardo Serra[2]

[1]Department of Informatics, Modelling, Electronics and Systems, University of Calabria, Cosenza, Italy, [2]Department of Computer Science, Boise State University, Boise, ID, United States

KEYWORDS

Internet of Things, security, privacy, mobile, network

Editorial on the Research Topic
Security and privacy for the Internet of Things

IoT devices represent one of the major targets for malicious activities. The grounds for this are manifold: first, since security requires investments, for commercial reasons, manufacturers may sell vulnerable products, leaving users with security concerns that are unlikely to be fixed. Second, many IoT devices lack the processing power to execute security software or even permit its installation. Third, the heterogeneity of applications, hardware, and software widens the attack surface while also making the implementation of comprehensive security solutions more difficult.

As a result, IoT networks are subject to a variety of cyber threats coming from the Internet as well as from other infected IoT devices, such as denial of service attacks, information theft, ransomware, and cryptominers. To counter such a variety of attacks, the IoT calls for security and privacy-preserving technologies, such as intrusion prevention, detection and reaction systems, and privacy-preserving protocols, that, with the proliferation of IoT devices in everyday life, have become a critical requirement.

This Research Topic focuses on the recent advances in the area of security and privacy solutions for the IoT. It consists of four papers that were selected by experts *via* a peer-review process. In the following, we summarize these articles and highlight their major contributions.

Ayres-Pereira et al. examine how various factors, such as the degree of e-privacy concerns and control over data access permissions, can influence a user's intention to install a smartphone app. They conducted two survey-based experiments with 441 participants and concluded that the type of app plays a central role in determining both the perceived benefit of installing the app and the level of e-privacy concerns. Finally, they discuss the implications of the achieved results regarding psychological factors involved in the app installation decision-making process and the importance of promoting data protection by design.

Saheed et al. propose a hybrid Autoencoder and Modified Particle Swarm Optimization algorithm for feature selection and a deep neural network (DNN) for the detection and classification of on-going attacks. The PSO with modification of inertia weight is utilized to optimize the parameters of the DNN. The findings obtained by analyzing the proposed solution against a generic attack in the UNSW-NB15 dataset gave high classification accuracy and detection rate.

Jairam et al. (in press) study whether a subset of features that embody human cognitive motor features can be used to identify a particular user with the aim of identifying intruders. They consider how security might be made more efficient by embodying Principal Component Analysis (PCA) into the interface, which has the potential to reduce the features utilized in the identification of intruders.

Hamoud and Aïmeur analyse different attack vectors examining the techniques used against end-users, who are targeted as a way of accessing larger organizations. They show how the information that is disclosed to social networks can be transformed to provide insights about an organization and the role of the victim in this process. The proposed model is a solution to help organizations establish security-conscious behaviors among their employees.

Author contributions

All authors listed have made a substantial, direct, and intellectual contribution to the work and approved it for publication.

Reference

Jairam, A., Halevi, T., and Raphan, T. Machine learning methods for improving mobile device security: a behavioral biometric approach. *Front. Comput. Sci.* (in press) 42.

Conflict of interest

The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Publisher's note