

Call for Papers for a Special Section on
**Artificial Intelligence for Security
and Privacy**

<http://toit.acm.org/announcements.cfm>



**ACM Transactions on
Internet Technology**

Special Section Editors

[Natalia Criado](#)

King's College London
natalia.criado@kcl.ac.uk

[Ozgur Kafali](#)

North Carolina State University
rkafali@ncsu.edu

[Martin Rehak](#)

Cisco Systems, Czech Republic
marrehak@cisco.com

[Jose. M Such](#)

Lancaster University
j.such@lancaster.ac.uk

[Pinar Yolum](#)

Bogazici University
pinar.yolum@boun.edu.tr

Send generic questions about the
special section to
acm.toit.ai4sp@gmail.com

Deadlines

Submission: 3 October 2016
First decision: 17 January 2017
Revision: 3 March 2017
Final decision: 3 May 2017
Final: 3 June 2017
Publication: 31 October 2017

Submission

<http://toit.acm.org/authors.cfm>
Please select "Special Section:
Artificial Intelligence for Security and
Privacy" under Manuscript Type
dropdown in the Manuscript Central
website.

Security and privacy are of capital importance to the development of a sustainable, resilient and prosperous cyber world. This includes protecting crucial assets ranging from Critical Infrastructures to individual's Personal Information, and it spans domains like Cloud computing, Social Computing, Electronic Commerce and many more. Approaches that are intelligent and self-adaptable are required to deal with the complexities of effectively protecting these crucial assets in all these domains. This is where research from the Artificial Intelligence community can make a difference in security and privacy.

The focus of this ToIT special section is to provide a forum to discuss and advance security and privacy by means of *AI approaches*. A list of topics to be covered by this special section includes, but is not limited to a set of areas listed below.

Models

- Game-theory
- Trust
- Norms and normative systems
- Organisations
- Human factors
- Data science
- Information theory
- Verification / model checking

Methods

- Access control
- Adversarial/ insider threat modelling
- Human behaviour modelling
- Security and privacy policies
- Risk assessment and management, and risk mitigation strategies
- Digital forensics
- Intrusion detection/prevention systems
- Automated vulnerability assessment
- Mining and visualization of large volumes of highly dynamic data

Technologies

- Cloud computing
- Social software / social computing
- Online Social Networks
- Internet of Things / Cyber-physical systems
- Critical infrastructures
- Linked Data
- Big Data