The 14th International Workshop on Cyberspace Security and Artificial Intelligence (CAI-2022)

To be held in conjunction with IEEE TrustCom-2022, 28-30 October 2022, Wuhan, China

Highlights:
- One Best Workshop Paper Award will be selected.
- Paper submission deadline (extended): 31 July 2022

Introduction

============

With the fast development of 5G/6G, Internet of Things (IoT), Cloud/Edge Computing, and Industry 4.0/5.0, Cyberspace Security is of paramount importance and has become a burning issue that may hinder the deployment of many innovative business models. Artificial Intelligence (AI) has been penetrated into many sectors, e.g., manufacturing, energy and health, to facilitate automation on trust, security, resilience and reliability. In addition, many of the applications in these sectors, such as self-driving cars and remote surgery, are critical and high stakes applications. The opaque decision making, and bias and ethical issues of AI challenge the safety of these applications. Cyberspace Safety has therefore been attracting significant attention in recent years.

This workshop will address the important problems and challenges caused by both AI for Cyberspace Security and Cyberspace Security for AI. The workshop aims to bring together computer scientists and engineers in different disciplines to share and exchange their experience and ideas and discuss state-of-the-art and in-progress research on all aspects of cyberspace security and AI.

This CAI workshop stemmed from the International Workshop on Security in e-Science and e-Research (ISSR). This year's event has the core theme of AI-powered Cyberspace Security and Safety, previously held as CAI-21 (held in New York, USA, in conjunction with ISPA 2021), ISSR-20 (held in Nanjing, China, in conjunction with SpaCCS 2020), ISSR-19 (held in Atlanta, USA, in conjunction with SpaCCS 2019), ISSR-18 (held in Melbourne, Australia, in conjunction with SpaCCS 2018), ISSR-17 (held in Guangzhou, China, in conjunction with SpaCCS 2017), ISSR-16 (held in Zhangjiajie, China, in conjunction with SpaCCS 2016), ISSR-15 (held in Columbus, USA, in conjunction with IEEE ICDCS-15), ISSR-14 (held in Vasteras, Sweden, in conjunction with IEEE COMPSAC-14), ISSR-13 (held in Melbourne, Australia, in conjunction with IEEE TrustCom-13), ISSR-12 (held in Liverpool, UK, in conjunction with IEEE TrustCom-12), ISSR-11 (held in Changsha, China, in conjunction with IEEE TrustCom-11), ISSR-10 (held in Taipei, Taiwan, in conjunction with IEEE ISPA-10) and ISSR-09 (held in Chengdu, China, in conjunction with IEEE ISPA-09).

We solicit original papers reporting a wide spectrum of topics related to cyberspace security and AI. Topics of interest include but are not limited to:

- Explainable machine learning for cyberspace security and safety
- Human machine intelligence for cyberspace security and safety
- Adversarial machine learning

- Security and safety for autonomous systems
- Security and safety for embedded systems
- Digital twins and cyberspace security
- Game theoretic reasoning in cyberspace security and safety
- SDN security and safety
- Cloud security and AI
- Smart contract security and safety
- Lightweight security and safety
- Network intrusion detection and safety
- Post quantum security and safety
- Trust management and safety
- Privacy and data protection
- AI for cyberspace security and safety
- Self-healing for cyberspace security and safety
- Automotive cyber security and safety
- Secure AI modeling and architecture
- Novel cryptographic mechanism for AI
- Security protocols for AI
- Security and safety in data mining and analytics
- Attack and defense methods with adversarial example
- Cyberspace security and safety for 5G/6G
- Cyberspace security and safety for internet of things
- Cyberspace security and safety for industry 4.0/5.0
- Smart grid security and safety
- Applications of AI for cyberspace security and safety
- Security issues of federated learning

Important Dates
===============

Submission Deadline: 31 July 2022
Authors Notification: 15 August 2022
Camera-Ready Paper Due: 15 September 2022
Registration Due: 22 September 2022

Paper Submission Guideline
==========================

Prospective authors are invited to submit manuscripts reporting original unpublished research and recent developments in the topics related to the workshop. The length of the papers should not exceed 6 pages + up to 4 pages for overlength charges (IEEE Computer Society Proceedings Manuscripts style: two columns, single-spaced, 10-point font), including figures and references.

The template files for LATEX or WORD can be downloaded:
https://www.ieee.org/conferences/publishing/templates.html

Papers should be submitted through the EDAS - https://edas.info/N29931

All papers will be peer reviewed and the comments will be provided to the authors. Once accepted, the paper will be included into the IEEE conference proceedings published by IEEE Computer Society Press (indexed by EI).

Submission of a paper should be regarded as an undertaking that, should the paper be accepted, at least one of the authors will register for the conference and present the work.

Organizing Committee
====================

General Co-Chairs
Chunhua Su, University of Aizu, Japan
Gautam Srivastava, Brandon University, Canada
Shui Yu, University of Technology Sydney, Australia

Program Co-Chairs
Lexi Xu, China Unicom, China
Vasileios Vasilakis, University of York, UK
Guodong Wang, Massachusetts College of Liberal Arts, USA
Xiaojun Zhai, University of Essex, UK

Steering Committee
Yulei Wu, University of Exeter, UK (Chair)
Guojun Wang, Guangzhou University, China (Chair)
Richard Hill, University of Huddersfield, UK
Wei Jie, University of West London, UK
Ryan Ko, University of Queensland, Australia
Xuejia Lai, Shanghai Jiao Tong University, China
Victor Leung, Shenzhen University, China / The University of British Columbia, Canada
Yi Pan, Shenzhen Institute of Advanced Technology, Chinese Academy of Sciences, China / Georgia State University, USA
Kouichi Sakurai, Kyushu University, Japan
Yang Xiang, Swinburne University of Technology, Australia
Zheng Yan, Xidian University, China/Aalto University, Finland
Albert Zomaya, The University of Sydney, Australia

Technical Program Committee
Roberto Canonico, University of Napoli Federico II, Italy
Yue Cao, Wuhan University, China
Yu Chen, San Jose State University, USA
Volkan Dedeoglu, CSIRO, Australia
Ralph Deters, University of Saskatchewan, Canada
Jinguang Han, Southeast University, China
Yi Han, Wuhan University of Technology, China
Xin Hu, Beijing University of Posts and Telecommunications, China
Jan Jürjens, University Koblenz & Fraunhofer ISST, Germany
Shahin Kamali, University of Manitoba, Canada

Sokratis Katsikas, Norwegian University of Science and Technology, Norway
Junichi Kishigami, Muroran Institute of Technology, Japan
Hong Li, Institute of Information Engineering, Chinese Academy of Sciences, China
Jing Li, University of Houston, USA
Jun Li, Nanjing University of Science and Technology, China
Yangzhe Liao, Wuhan University of Technology, China
Wansu Lim, Kumoh National Institute of Technology, South Korea
Gao Liu, Xidian University, China
Jiqiang Liu, Beijing Jiao Tong University, China
Chengnian Long, Shanghai Jiao Tong University, China
Hassan Mahdikhani, University of New Brunswick, Canada
John Palfreyman, Palfreyman Ventures, United Kingdom
Sarada Prasad Gochhayat, University of Padua, Italy
Yi Ren, University of East Anglia, United Kingdom
Laura Ricci, University of Pisa, Italy
Björn Scheuermann, TU Darmstadt, Germany
Hirotsugu Seike, The University of Tokyo, Japan
Abhishek Singh, IBM India Research Laboratory, India
Wangyang Yu, Shaanxi Normal University, China
Qianyun Zhang, Beihang University, China

For any queries, please contact Yulei Wu (y.l.wu@exeter.ac.uk) and Guojun Wang (csgjwang@gzhu.edu.cn)