

**CALL FOR PAPERS**

**The 12th Pacific Asia Workshop on Intelligence and Security Informatics**

**PAISI 2017**

**(to be held in conjunction with PAKDD 2017)**

**Workshop Website: <http://www.business.hku.hk/paisi/2017/>**

**May 23, 2017, Jeju Island, South Korea**

**Important Dates**

- Submission due **December 31, 2016**
- Notification of acceptance **January 27, 2017**
- Camera-ready copy due **February 10, 2017**

**Workshop Scope**

Intelligence and Security Informatics (ISI) is concerned with the study of the development and use of advanced information technologies and systems for national, international, and societal security-related applications. The annual IEEE International Conference series on ISI was started in 2003. In 2006, the Workshop on ISI was started in Singapore in conjunction with PAKDD, with most contributors and participants from the Pacific Asian region. Since then, PAISI was held annually in Chengdu (2007), Taipei (2008), Bangkok (2009), Hyderabad (2010), Beijing (2011), Kuala Lumpur (2012), Beijing (2013), Tainan (2014), Ho Chi Minh City (2015), and Auckland (2016). This year PAISI 2017 will once again be held in conjunction with PAKDD (<http://pakdd2017.pakdd.org>) and will provide a stimulating forum for ISI researchers in Pacific Asia and other regions of the world to exchange ideas and report research progress.

**Paper Submission/Areas of Interest**

Submissions may include systems, methodology, testbed, modeling, evaluation, and policy papers. Topics include but are not limited to:

<b>I. Information Sharing and Big Data Analytics</b>	<b>II. Infrastructure Protection and Emergency Responses</b>	<b>III. Cybercrime and Terrorism Informatics and Analytics</b>	<b>IV. Enterprise Risk Management, IS Security, and Social Media Analytics</b>
<ul style="list-style-type: none"> <li>• Intelligence-related knowledge discovery</li> <li>• Big data analytics and mining</li> <li>• Criminal data mining and network analysis</li> <li>• Criminal/intelligence information sharing and visualization</li> <li>• Web-based intelligence monitoring and analysis</li> <li>• Spatio-temporal data analysis/GIS for crime analysis and security informatics</li> <li>• Cyber-crime detection and analysis</li> <li>• Authorship analysis and identification</li> <li>• Privacy and civil liberties issues</li> <li>• Text processing and mining</li> </ul>	<ul style="list-style-type: none"> <li>• Public health and bioterrorism information infrastructure</li> <li>• Transportation and communication infrastructure protection</li> <li>• Cyber-infrastructure design and protection</li> <li>• Intrusion detection</li> <li>• Border/transportation safety</li> <li>• Emergency response and management</li> <li>• Disaster prevention, detection, and management</li> <li>• Communication and decision support for search and rescue</li> <li>• Infrastructure for big data analytics</li> </ul>	<ul style="list-style-type: none"> <li>• Cyber-crime and social impacts</li> <li>• Terrorism related analytical methodologies and software tools</li> <li>• Terrorism knowledge portals and databases</li> <li>• Social network analysis (radicalization, recruitment, conducting operations), visualization, and simulation</li> <li>• Forecasting terrorism</li> <li>• Countering terrorism</li> <li>• Measuring the impact of terrorism on society</li> <li>• Computer forensics</li> </ul>	<ul style="list-style-type: none"> <li>• Information systems security policies</li> <li>• Behavior issues in information systems security</li> <li>• Fraud detection and deception detection</li> <li>• Viruses and malware</li> <li>• Corporate going concerns and risks</li> <li>• Accounting and IT auditing</li> <li>• Corporate governance and monitoring</li> <li>• Board activism and influence</li> <li>• Corporate sentiment surveillance</li> <li>• Market influence analytics and media intelligence</li> <li>• Consumer-generated media and social media analytics</li> </ul>

Long papers (20 pages) and short papers (10 pages) in English may be submitted electronically via the online submission site (<http://www.easychair.org/conferences/?conf=paisi2017>). Submission file formats are PDF, Microsoft Word, or LaTeX. Submitting a paper to the workshop means that if the paper is accepted, at least one author should attend the workshop to present the paper. All accepted PAISI 2017 papers will be published in Springer's Lecture Notes in Computer Science (LNCS) series, same as all past PAISI proceedings. Required LNCS Microsoft Word/LaTeX templates can be found on the workshop website.

**Hosts and Sponsors**

The University of Arizona, The University of Hong Kong, Virginia Tech

**Workshop Organizing Co-chairs**

G. Alan Wang, Virginia Tech  
Michael Chau, The University of Hong Kong  
Hsinchun Chen, The University of Arizona