

**Pacific Asia Workshop on Intelligence and Security Informatics  
PAISI 2010**

**(to be held in conjunction with PAKDD 2010)  
Workshop Website: <http://www.business.hku.hk/paisi/>  
June 21, 2010, Hyderabad, India**

**Important Dates**

- Submission due February 20, 2010
- Notification of acceptance March 20, 2010
- Camera-ready copy due March 30, 2010

**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. The 2nd PAISI was then held in Chengdu in 2007, the 3rd PAISI was held in conjunction with IEEE ISI in Taipei in 2008, and the 4th PAISI was held in conjunction with PAKDD in Bangkok in 2009. This year, PAISI 2010 will once again be held with PAKDD 2010 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. The workshop also welcomes contributions dealing with ISI challenges specific to the Pacific Asian region.

**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 Data/Text Mining</b>	<b>II. Infrastructure Protection and Emergency Responses</b>	<b>III. Terrorism Informatics</b>	<b>IV. Enterprise Risk Management and Information Systems Security</b>
<ul style="list-style-type: none"> <li>• Intelligence-related knowledge discovery</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>• Deception and intent detection</li> <li>• Cyber-crime detection and analysis</li> <li>• Authorship analysis and identification</li> <li>• Applications of digital library technologies in intelligence data processing, preservation, sharing, and analysis</li> <li>• Agents and collaborative systems for intelligence sharing</li> <li>• HCI and user interfaces of relevance to intelligence and security</li> <li>• Information sharing policy and governance</li> <li>• Privacy and civil liberties issues</li> </ul>	<ul style="list-style-type: none"> <li>• Public/animal 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>• Assisting citizens' responses to terrorism and catastrophic events</li> </ul>	<ul style="list-style-type: none"> <li>• Terrorism related analytical methodologies and software tools</li> <li>• Terrorism knowledge portals and databases</li> <li>• Terrorist incident chronology databases</li> <li>• Terrorism root cause analysis</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>• Measuring the effectiveness of counter-terrorism campaigns</li> </ul>	<ul style="list-style-type: none"> <li>• Information security management standards</li> <li>• Information systems security policies</li> <li>• Behavior issues in information systems security</li> <li>• Fraud detection</li> <li>• Cyber crime and social impacts</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 (12-page) and short (6-page) papers following the Springer LNCS paper templates in English may be submitted electronically via the online submission site (<http://www.easychair.org/conferences/?conf=paisi2010>). Submission file formats are PDF, Microsoft Word, or LaTeX. We are in the process of making arrangements with Springer to publish accepted PAISI 2010 papers in its Lecture Notes in Computer Science (LNCS) series, as for PAISI 2009, PAISI 2008, PAISI2007, and WISI2006. Required LNCS Microsoft Word/LaTeX templates can be found on the workshop website. Authors who wish to only present a poster may submit a 2-page extended abstract, which will be reviewed and will appear in the Proceedings if accepted.

**Hosts and Sponsors**

The University of Arizona, USA                      The University of Hong Kong                      The University of Mysore, India

**Workshop Organizing Co-chairs**

Hsinchun Chen, The University of Arizona, USA  
Michael Chau, The University of Hong Kong  
Shu-hsing Li, National Taiwan University  
Shalini Urs, University of Mysore, India

**Program Co-chairs**

Srinath Srinivasa, IIT-Bangalore, India  
G. Alan Wang, Virginia Tech, USA