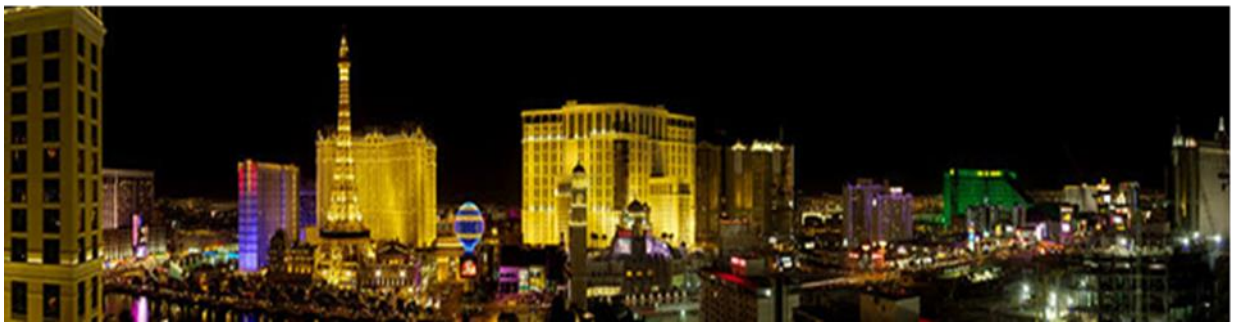

Intelligent Computing and Cyber Security

A Special Track of the
10th International Symposium on Visual Computing (ISVC14)

http://www.isvc.net

December 8-10, 2014
Las Vegas, Nevada, USA

Scope:

Rapid growth in networking, computation, software and hardware technologies have revolutionized the cyberspace landscape. From simple record keeping and day-to-day communications to military operations and highly secured business transactions are performed using networked systems enabled with remote access technologies. Thus the cyberspace has become an integral part of our daily lives; especially when we are living in a virtual world built on top of social networks, cloud infrastructure, and smart mobile devices.

Cyber-attacks are currently prevailing in all these cyberspaces, user networking devices, and the applications. They are even more complex and malicious in the distributed and mobile environment. Securing the cyberspace infrastructure is thus not only necessary but also has become a critical priority to ensure proper functioning of the cyberspace, smart grids, economic growth and advancement in the technologies.

Owing to its powerful analytical and modeling frameworks, Artificial Intelligence, Machine Learning, Behavioral Learning, Pattern Recognition have recently emerged as key tools for building automated, resilient, secure, and dependable cyber systems. This track will focus on identifying such novel and state of the art solutions to problems related to cyber security. The goal of this special track is to bring together researchers and practitioners from academia, industry, and government agencies to focus on understanding modern cyber security threats and countermeasures, and establishing original contributions and new collaborations in these areas.

Topics:

The topics of interest include but are not limited to the following areas:

- Data mining for critical infrastructure security
- Machine learning for intrusion prevention/detection systems
- Pattern recognition and anomaly detection
- AI and cloud computing security
- Machine learning and cognitive radio networking security
- Game theory, learning and decision theory for cybersecurity
- Machine learning and pattern recognition in covert communications
- Empirical and experimental analyses and simulation studies
- Automated exploitation tools and analyses
- Machine learning and prediction in malware analysis
- AI & Network Systems security
- NLP for text analysis in Cyber Security
- Threat monitoring and analysis
- Trusted networking security and privacy

Paper Submission Procedure:

Papers submitted to ISVC 2014 Special Track must not have been previously published and must not be currently under consideration for publication elsewhere. Manuscripts should not exceed 12 pages, including figures and tables (see http://www.isvc.net for details). All papers accepted will appear in the symposium proceedings which will be published by Springer-Verlag in the Lecture Notes in Computer Science (LNCS) series.

Important dates:

Paper submission:	August 23, 2014
Notification of acceptance:	October 7, 2014
Final camera-ready paper:	October 31, 2014
Advance Registration:	October 31, 2014
ISVC14 Symposium:	December 8-10, 2014

Organizers:

Shamik Sengupta, University of Nevada, Reno, NV, USA, ssengupta@unr.edu
Ming Li, University of Nevada, Reno, NV, USA, ml845@msstate.edu
Yoohwan Kim, University of Nevada, Las Vegas, NV, USA, Yoohwan.Kim@unlv.edu
Juyeon Jo, University of Nevada, Las Vegas, NV, USA, joj5@unlv.nevada.edu