IEEE Symposium Series on Computational Intelligence 2018
Special Session on "Computational Intelligence in Cyber Threat Analytics"

Organizers: **Vinti Agarwal, Katrin Franke, Andrii Shalaginov, M. Tanveer**

Aim and Scope: In the last couple of years, the growing demand for digitalization in society has led to the increase in computational capabilities, volume of data, and as a result to more cyber threats. Artificial and computational intelligence has attained a huge popularity in providing solutions to the numerous challenges arising in the field of computer vision, natural language processing, knowledge management, decision making, *etc.*. But, less has been contributed towards the area of cyber threat intelligence (CTI) to uncover cyber attacks and cyber espionage to the information and communication technology in real-time. Recently, cyber security experts and digital forensic analysts have been facing big challenges in providing adaptive and timely response for new and unknown threats to the decision makers. To address this problem, computational intelligence algorithms can be used to design effective and efficient methods to collect, structure and analyze sheer volume of threat data enabling identification of threat actors, their behaviors, resources, and attack methodologies.

By combining data from multiple sources (also termed as data fusion or data enrichment), computational intelligence can further boost the performance of traditional cyber security protection and response methods. The main objective of applying computational intelligence in cyber threat analytics is to establish correlation between different cyber events, utilize historical information to detect threat patterns, trends, and anomalies in the threat data. This helps in providing more sophisticated, targeted, and tailored threat alerts, by adding context to these alerts. Further, it enables industry and government organizations to increase the quality of their decisions regarding particular threat alerts. As result, performance and reliability of decision support systems in cyber incidents handling can be considerably improved.

Topics: This special issue focuses on sharing recent advances in computational intelligence, machine learning techniques, algorithms, methods and tools to perceive, reason, learn and act on a wide range of cyber threat data available from multiple sources such as malware campaigns, network attacks, HackForums[1], LeakForums[2], Darknets etc.

[1] `https://hackforums.net/`
[2] `https://leakforums.net/`

Topics appropriate for this special issue include novel supervised, unsupervised, semi-supervised and reinforcement machine learning algorithms, new formulations, and applications in cyber threat intelligence (but are not necessarily limited to):

- Open source threat intelligence data-driven methods.
- Methods and models for cyber threat graphs representation learning.
- Heterogeneous data and machine learning model fusion.
- Machine learning based recommender systems for CTI.
- Open source social media intelligence (OSSMINT) for government and law enforcement agencies. (*i.e.* Illegal trading of products & services, online radicalization, revealing terrorist threats and extremism *etc.*)
- Malware entity identification and classifications.
- Potential threat actors and their suspicious behavior modelling.
- Machine learning in intrusion detection systems, mitigation and response techniques.
- Cyber threat predictive analysis on virtual security products.
- Algorithms/Platforms for sharing and exchange cyber threat knowledge.
- Privacy-preserving approaches to cyber threat intelligence information release.
- Threat actors, tactics, techniques, relationships and behavior modelling using PRE-ATT&CK Matrix & MISP Galaxy clusters.

Submission Guidelines: The submission guidelines are adopted from the main conference. Authors are required to submit their manuscripts for this special session at the regular paper submission website `http://ieee-ssci2018.org/submission.html`. Papers should not exceed a maximum of 8 pages (including abstract, body, tables, figures, and references), and should be submitted, written in English, as a pdf in 2-column IEEE format. Detailed instructions for submitting papers are provided on the conference at home page.

Only technical papers describing previously unpublished, original, state-of-the-art research, and not currently under review by a conference or a journal will be considered for publication. Extended work must have a significant number of "new and original" contributions along with more than 60 percent brand "new" material. All accepted papers must be presented by at least one of the authors to be published in the electronic proceedings of the conference in IEEE Xplore Digital Library.

Important Dates:
Paper Submission Deadline: **June 15, 2018**
Decision: **August 15, 2018**
Early Bird Registration: **September 15, 2018**

Contact Information
Please, do not hesitate to contact us for more information at: vinti.agarwal@ntnu.no

Biography of the organizers:

Dr. Vinti Agarwal is a postdoctoral researcher in the Digital Forensic Group in the Department of Information Security and Communication Technology at Norwegian University of Science and Technology (NTNU). Currently, she is working with Professor Katrin Franke and Professor Slobodan Petrovic on ACT funded project in collaboration with Mnemonic AS, Oslo. Her research interest lies in domains of social network analysis and mining, recommender systems, social computing, machine learning, and cyber security. She received her doctorate degree in the field of machine learning and social network analysis at Artificial Intelligence Lab in JawaharLal Nehru University, New Delhi, India in January, 2016. During Ph.D., she was majorly focussed towards applying machine learning techniques to model and design social recommender systems, by mining large scale social data, to help users in finding potentially new friends and organizing existing friends into various groups on social networking sites. She completed her M.Tech. in Computer Science and Engineering from Jawaharlal Nehru University, India in July 2011 and was awarded full-time senior research fellowship by Council of Scientific and Industrial Research, a premier national R&D organization.
Official Homepage: `https://www.ntnu.edu/employees/vinti.agarwal`

Dr. Katrin Franke is professor of computer science at the NTNU Digital Forensics Group at the Norwegian University of Science and Technology (NTNU). In 2005 she obtained her Ph.D. degree at the Artificial Intelligence Institute, University of Groningen, The Netherlands. She is an alumni of the Technical University of Dresden in Germany with a degree in Electrical Engineering. After graduating in 1994, Dr. Franke began to conduct research at the Fraunhofer IPK in Berlin, Germany. Until December 2006, she has worked as a scientific project manager; leading research teams as well as internationally distributed project consortia. In 2007 Katrin Franke joined the Norwegian Information Security laboratory at Gjøvik University College in Norway, now NTNU Department of Information Security and Communication Technology (IIK). She conducts research in Computational Forensics, supervises Ph.D. projects and teaches courses in Machine Learning and Pattern Recognition at the PhD and master level. Dr. Franke has published more than 180 scientific articles including one patent. She is involved in the organization of international conferences; the most prominent among them is the International Workshop on Computational Forensics (IWCF). Dr. Franke is a founding member of the IAPR-TC6 on Computational Forensics founded in 2008 and served as its chair. Katrin Franke is an IAPR* Young Investigator Awardee in the year 2009. (* International Association of Pattern Recognition)
Official Homepage: `https://www.ntnu.no/ansatte/katrin.franke`

Dr. Andrii Shalaginov is a postdoctoral research fellow in Digital Forensics at the the Department of Information Security and Communication Technology (Digital Forensics Group), Faculty of Information Technology and Electrical Engineering, Norwegian University of Science and Technology (NTNU). Andrii has been awarded with PhD degree in Information Security from NTNU in February 2018. His PhD research was devoted to development of new Soft Computing methods for Digital Forensics applications. Also during the last seven years, Andrii has been working with malware research. His primary expertise is in static and dynamic malware analysis, development of machine learning-aided intelligent computer viruses detection models and similarity-based

categorization of malware types and families. By now, Andrii received his 2nd Master Degree in Information Security (Digital Forensics) from the Gjøvik University College (GUC) in 2013 and also holds BSc (2009) and 1st MSc (2011) degrees in System Designing from the National Technical University of Ukraine "Kyiv Polytechnic Institute" - Department of Computer Aided Design. Before starting at GUC he had an industry experience, including Samsung R&D Center.
Official Homepage: `https://www.ntnu.edu/employees/andrii.shalaginov`

Dr. Mohammad Tanveer is Assistant Professor and Ramanujan Fellow at the Discipline of Mathematics of the Indian Institute of Technology, Indore. Prior to that, he spent one year as a Postdoctoral Research Fellow at the Rolls-Royce@NTU Corporate Lab of the Nanyang Technological University, Singapore. He received the Ph.D degree in Computer Science from the Jawaharlal Nehru University, New Delhi, India, where he was advised by Professor S. Balasundaram. Prior to that, he received the M.Phil degree in Mathematics from Aligarh Muslim University, Aligarh, India, where he was advised by Prof. M. Imdad. His research interests include support vector machines, optimization, applications to Alzheimer's disease and dementias, biomedical signal processing, and fixed point theory and applications. He has published over 25 referred journal papers of international repute. He is the recipient of the 2016 DST-Ramanujan Fellowship in Mathematical Sciences and 2017 SERB-Early Career Research Award in Engineering Sciences which are the prestigious awards of INDIA at early career level. He has organized two international conferences and delivered many invited talks. He is a member of the editorial review board of Applied Intelligence, Springer (International Journal of Artificial Intelligence, Neural Networks, and Complex Problem-Solving Technologies). Dr. Tanveer is currently the Principal Investigator of 04 major research projects funded by Government of India including Department of Science and Technology (DST), Science & Engineering Research Board (SERB) and Council of Scientific & Industrial Research (CSIR).
Official Homepage: `http://www.iiti.ac.in/people/~mtanveer`