ICDCSW 2017

IEEE 37th International Conference on Distributed Computing Systems Workshops

June 5, 2017
Atlanta, USA

Editors
Dr. Aibek Musaev
University of Alabama, USA

Dr. Joao E. Ferreira
University of Sao Paulo, Brazil

Dr. Teruo Higashino
University of Osaka, Japan
# Table of Contents

- Workshops Hotel Floor Plan ........................................................................................................... 4
- Message from the ICDCS 2017 Workshops Chairs ........................................................................... 5
- Organizing Committee ...................................................................................................................... 6
- Program at a Glance .......................................................................................................................... 7
- Schedule: Monday, June 5, 2017 ...................................................................................................... 8
- ADSN 2017 Workshop Abstracts ........................................................................................................ 15
- BGP 2017 Workshop Abstracts ......................................................................................................... 16
- CCN-CPS 2017 Workshop Abstracts ................................................................................................. 18
- HotPOST 2017 Workshop Abstracts .................................................................................................. 21
- IoTCA 2017 Workshop Abstracts ...................................................................................................... 23
- JCC 2017 Workshop Abstracts .......................................................................................................... 25
- PED 2017 Workshop Abstracts ......................................................................................................... 28
- PSBD 2017 Workshop Abstracts ........................................................................................................ 29
- WoSC 2017 Workshop Abstracts ...................................................................................................... 30
- NSF-JST 2017 Workshop Abstracts .................................................................................................. 31
- Local Information ............................................................................................................................... 32
Workshops Hotel Floor Plan

**Second Floor**
- Salon V
- Salon III
- Salon I
- Phoenix
- Ballroom
- Salon VI
- Salon IV
- Salon II

**Third Floor**
- Augusta
- Lexington
- Savannah

- Richmond
- Tallahassee

- Columbia
- Foyer
- Atlanta
- Coat Room
- Registration

- Charleston 2
- Staircase / Elevator
- Charleston 1

- Nashville
- Montgomery

- Elevators
- Frankfurt
- Jackson

**Meeting Rooms are not drawn to scale**

---

**JW MARRIOTT**
**ATLANTA BUCKHEAD**
Message from the ICDCS 2017 Workshops Chairs

It is great honor for us to welcome to the 10 workshops to be held along with the 37th IEEE International Conference on Distributed Computing Systems, ICDCS 2017 in Atlanta, GA, USA on June 5 – 8, 2017.

The ICDCS 2017 edition includes the following international workshops: the 16th International Workshop on Assurance in Distributed Systems and Networks, ADSN2017, the 9th International Workshop on Hot Topics in Planet-Scale Mobile Computing and Online Social Networking, HotPOST’17, the 8th International Workshop on Joint Cloud Computing, JCC2017, the 2nd International Workshop on Communication, Computing, and Networking in Cyber Physical Systems, CCN-CPS 2017, the International Workshop on Privacy and Security in Big Data EcoSystem, PSBD 2017, the 1st International Workshop on Integrating Process-oriented, Event-based and Data-driven Systems, ICDCS-PED 2017, the International Workshop on the Internet of Things Computing and Applications, IoTCA 2017, the 1st International Workshop on Serverless Computing, WoSC 2017, the International Workshop on Big Graph Processing, BGP 2017 and the 1st US-Japan Workshop on Collaborative Global Research on Applying Information Technology. We would like to thank all of the workshop organizers who proposed and held workshops. Without their efforts, we would not have been able to provide high-quality workshops.

We would also like to thank to the ICDCS 2017 organizers, especially for General Co-Chairs Calton Pu, Masaru Kitsuregawa, Karl Aberer and the Program Chair Ling Liu who kindly supported our efforts for success of the ten workshops.

Finally, we hope that ICDCS 2017 Workshops provide a stimulating forum for developing new ideas in emerging fields covered by the 10 workshops.

Workshops Chairs

Joao E. Ferreira, University of Sao Paulo, Brazil

Teruo Higashino, University of Osaka, Japan
Organizing Committee

Workshops Program Chairs
Joao E. Ferreira, University of Sao Paulo, Brazil
Teruo Higashino, University of Osaka, Japan

Workshops Publication Chair
Aibek Musaev, University of Alabama, USA

Finance Manager (non-volunteer, reporting to ICDCS General Chairs)
Carrie Stein, Ohio State University, USA
# Program at a Glance

**Monday, June 5, 2017**

<table>
<thead>
<tr>
<th>Time</th>
<th>Track 1 (Salon II)</th>
<th>Track 2 (Salon IV)</th>
<th>Track 3 (Salon VI)</th>
<th>Track 4 (Atlanta)</th>
<th>Track 5 (Columbia)</th>
<th>Track 6 (Savannah)</th>
</tr>
</thead>
<tbody>
<tr>
<td>7:00-8:00</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Continental Breakfast (Foyer)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8:00-9:30</td>
<td>Workshop: CCN-CPS</td>
<td>Workshop: HotPOST</td>
<td>Workshop: PSBD</td>
<td>Workshop: JCC</td>
<td>Workshop: NSF-JST Day 1</td>
<td></td>
</tr>
<tr>
<td>9:30-10:00</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Coffee Break (Foyer)</td>
</tr>
<tr>
<td>10:00-12:00</td>
<td>Workshop: CCN-CPS</td>
<td>Workshop: ADSN</td>
<td>Workshop: HotPOST</td>
<td>Workshop: PSBD</td>
<td>Workshop: JCC</td>
<td>Workshop: NSF-JST Day 1</td>
</tr>
<tr>
<td>12:00-13:30</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Lunch (Phoenix Ballroom)</td>
</tr>
<tr>
<td>15:30-16:00</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Coffee Break (Foyer)</td>
</tr>
<tr>
<td>16:00-17:00</td>
<td>Workshop: CCN-CPS</td>
<td>Workshop: ADSN</td>
<td>Workshop: PED-BGP</td>
<td>Workshop: IoTCA</td>
<td>Workshop: WoSC</td>
<td>Workshop: NSF-JST Day 1</td>
</tr>
<tr>
<td>17:00-18:00</td>
<td></td>
<td></td>
<td>Workshop: PED-BGP</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Schedule: Monday, June 5, 2017

Ten Workshops and two tutorials (see Program at a glance and workshops website and ICDCS 2017 website for details)

7:00-8:00 Monday, June 5, 2017

Continental Breakfast
Location: Foyer

8:00-9:30 Monday, June 5, 2017

Workshop: CCN-CPS, Session 1
Location: Salon II

Session Chair: Nader Mohamed (Middleware Technologies Lab.)

Policies Guiding Cohesive Interactions among Internet of Things with Communication Cloud and Social Networks
Henry Hexmoor (Southern Illinois University)

Enhanced Security of Building Automation Systems Through Microkernel-Based Controller Platforms
Xiaolong Wang (University of South Florida), Richard Habeeb (University of South Florida), Xinming Ou (University of South Florida), Siddharth Amaravadi (Kansas State University), John Hatcliff (Kansas State University), Masaaki Mizuno (Kansas State University), Mitchell L Neilsen (Kansas State University), Raj Rajagopalan (Honeywell), Srivatsan Varadarajan (Honeywell Aerospace Advanced Technology Labs)

High level Design of a Home Autonomous System Based on Cyber Physical System Modeling
Basman Alhafidh (Florida Institute of Technology), William H. Allen (Florida Institute of Technology)

Workshop: HotPOST, Session 1
Location: Salon VI

Keynote Speech: A Markov Game Theoretic Approach for Power Grid Security
Charles A. Kamhoua (Air Force Research Laboratory)

Router-based Brokering for Surrogate Discovery in Edge Computing
Julien Gedeon (Technische Universität Darmstadt), Christian Meurisch (Technische Universität Darmstadt), Disha Bhat (Technische Universität Darmstadt), Michael Stein (Technische Universität Darmstadt), Lin Wang (Technische Universität Darmstadt), Max Mühlhäuser (Technische Universität Darmstadt)

Modeling the Spread of Influence for Independent Cascade Diffusion Process in Social Networks
Zesheng Chen (Indiana University - Purdue University Fort Wayne), Kurtis Taylor (Indiana University - Purdue University Fort Wayne)

Workshop: PSBD, Opening and Invited Talks
Location: Atlanta

Keynote Speech: Big Data - Security and Privacy (and Transparency)
Elisa Bertino (Purdue University)

Invited Talk: Supporting Time-varying Privacy with Self-emerging Data
Balaji Palanisamy (University of Pittsburgh)

Workshop: JCC, Session 1
Location: Columbia

Heterogeneous Malware Spread Process in Star Network
Libo Jiao (Tsinghua University), Hao Yin (Tsinghua University), Dongchao Guo (Tsinghua University), Yongqiang Lyu (Tsinghua University)

Cost Reduction in Hybrid Clouds for Enterprise Computing
Biyu Zhou (Institute of Computing Technology, Chinese Academy of Sciences), Fa Zhang (Institute of Computing Technology, Chinese Academy of Sciences), Jie Wu (Temple University), Zhiyong Liu (Institute of Computing Technology, Chinese Academy of Sciences)

DC-RSF: A Dynamic and Customized Reputation System Framework for Joint Cloud Computing
Fanghua Ye (Sun Yat-sen University), Zibin Zheng (Sun Yat-sen University), Chuan Chen (Sun Yat-sen University), Yuren Zhou (Sun Yat-sen University)

Web Service Appliance Based on Unikernel
Kai Yu (National Lab for Parallel and Distributed Processing), Chengfei Zhang (National Lab for Parallel and Distributed Processing), Yunxiang Zhao (National Lab for Parallel and Distributed Processing)

Analysis and Evaluation of the GAS Model for Distributed Graph Computation
Wang Jinyan (National Lab for Parallel and Distributed Processing), Zhang Chengfei (National Lab for Parallel and Distributed Processing)

Traffic Signs Detection Based on Faster R-CNN
Zhongrong Zuo (National Lab for Parallel and Distributed Processing), Kai Yu (National Lab for Parallel and Distributed Processing), Qiao Zhou (National Lab for Parallel and Distributed Processing), Xu Wang (National Lab for Parallel and Distributed Processing), Ting Li (National Lab for Parallel and Distributed Processing)

JCLedger: A Blockchain Based Distributed Ledger for JointCloud Computing
Xiang Fu (National University of Defense Technology), Huaimin Wang (National University of Defense Technology), Peichang Shi (National University of Defense Technology), Yingwei Fu (National University of Defense Technology), Yijie Wang (National University of Defense Technology)

Corporation Architecture for Multiple Cloud Service Providers in JointCloud Computing
Peichang Shi (National University of Defense Technology), Huaimin Wang (National University of Defense Technology), Xikun Yue (National University of Defense Technology), Shilan Yang (National University of Defense Technology), Shangzhi Yang (National University of Defense Technology), Yuxing Peng (National University of Defense Technology)

Sharing Privacy Data in Semi-Trustworthy Storage through Hierarchical Access Control
Yuzhao Wu (Tsinghua University), Yongqiang Lyu (Tsinghua University), Qian Fang (Tsinghua University), Geng Zheng (Tsinghua University), Hao Yin (Tsinghua University), Yuanchun Shi (Tsinghua University)

Workshop: NSF-JST
Location: Savannah

9:30-10:00 Monday, June 5, 2017

Coffee Break
Location: Phoenix Ballroom

10:00-12:00 Monday, June 5, 2017

Workshop: CCN-CPS, Session 2
Location: Salon II

Session Chair: Jameela AlJaroodi (Robert Morris University)

A Cyber Physical Buses-and-Drones Mobile Edge Infrastructure for Large Scale Disaster Emergency Communications
Mamta Narang (Auckland University of Technology), William Liu (Auckland University of Technology), Jairo A Gutierrez (Auckland University of Technology), Luca Chiaraviglio (University of Rome Tor Vergata)

A Performance Comparison of Containers and Virtual Machines in Workload Migration Context
Kumar Gaurav (VMware Software India Pvt Ltd), Pavan Karkun (VMware Software India pvt LTD), Y. C. Tay (National University of Singapore)

Towards Service-Oriented Middleware for Cyber Physical Systems
Nader Mohamed (Middleware Technologies Lab.), Sanja Lazarova-Molnar (University of Southern Denmark)

Networking and Communication in Cyber Physical Systems
Imad Jawhar (UAE University), Jameela Al-Jaroodi (Robert Morris University)

Workshop: ADSN, Session 1: Keynote, Session 2: Assuring Temporal Fairness and Securing Communication
Location: Salon IV

Keynote Speech: Dependability Challenges in 5G Cellular Networks
Douglas M. Blough (Georgia Institute of Technology)
Understanding and Improving Temporal Fairness on an Electronic Trading Venue
Hayden Melton (Deakin University)

Certificate Less Cryptography-based Rule Management Protocol for Advanced Mission Delivery Networks
Jongho Won (Purdue University), Ankush Singla (Purdue University), Elisa Bertino (Purdue University)

Workshop: HotPOST, Session 2
Location: Salon VI

Thank You For Being A Friend: An Attacker View on Online-Social-Network-based Sybil Defenses
David Koll (University of Goettingen), Martin Schwarzaeir (University of Goettingen), Jun Li (University of Oregon), Xiang-Yang Li (University of Science and Technology of China), Xiaoming Fu (University of Goettingen)

Efficient Dynamic Service Function Chain Combination of Network Function Virtualization
Wenke Yan (Beijing University of Posts and Telecommunications), Konglin Zhu (Beijing University of Posts and Telecommunications), Lin Zhang (Beijing University of Posts and Telecommunications), Sixi Su (Beijing University of Posts and Telecommunications)

When Augmented Reality meets Big Data
Carlos Bermejo (The Hong Kong University of Science and Technology), Zhanpeng Huang (The Hong Kong University of Science and Technology), Tristan Braud (The Hong Kong University of Science and Technology), Pan Hui (The Hong Kong University of Science and Technology)

Sampling Based Efficient Algorithm to Estimate the Spectral Radius of Large Graphs
Samar Abbas (Lahore University of Management Sciences), Juvaria Tariq (Lahore University of Management Sciences), Arif Zaman (Lahore University of Management Sciences), Imdadullah Khan (Lahore University of Management Sciences)

Extemporaneous Micro-Mobile Service Execution Without Code Sharing
Zheng Song (Virginia Tech), Min Le (Utah State University), Young-Woo Kwon (Utah State University), Eli Tilevich (Virginia Tech)

Preventing Colluding Identity Clone Attacks in Online Social Networks
Georges A. Kamhoua (Florida International University), Niki Pissinou (Florida International University), S.S. Iyengar (Florida International University), Jonathan Beltran (Florida International University), Charles Kamhoua (Air Force Research Laboratory), Brandon L Hernandez (UTRGV), Laurent Njilla (Air Force Research Laboratory)

Workshop: PSBD, Research Session
Location: Atlanta

A novel game-theoretic model for content-adaptive image steganography
Qi Li (Hunan University), Xin Liao (Hunan University), Guoyong Chen (Hunan University), Liping Ding (Guangzhou Branch of Institute of Software, Chinese Academy of Science)

A Fine-grained Access Control Scheme for Big Data Based on Classification Attributes
Tengfei Yang (State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences), Peisong Shen (State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences), Xue Tian (State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences), Xi Chen (State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences)

Social-Aware Decentralization for Efficient and Secure Multi-Party Computation
Yuzhe Tang (Syracuse University), Sucheta Soundarajan (Syracuse University)

Statistical Anomaly Detection on Metadata Streams via Commodity Software to Protect Company
Christine Chen (University of Portland), James Gurganus (Micro Systems Engineering, Inc.)

Computational improvements in parallelized k-anonymous microaggregation of large databases
Ahmad Mohamad Mezher (Universitat Politècnica de Catalunya (UPC)), Alejandro García Álvarez (Universitat Politècnica de Catalunya (UPC)), David Rebollo-Monedero (Universitat Politècnica de Catalunya (UPC)), Jordi Forné (Universitat Politècnica de Catalunya (UPC))

Workshop: JCC, Session 2
Location: Columbia

A Reliability Benchmark for Big Data Systems on JointCloud
Yingying Zheng (Institute of Software, Chinese Academy of Sciences), Lijie Xu (Institute of Software, Chinese Academy of Sciences), Wei Wang (Institute of Software, Chinese Academy of Sciences), Wei Zhou (KSYUN), Ying Ding (Changchun University of Science and Technology)

UCPR: User Classification and Influence Analysis in Social Network
Cong Zha (Tsinghua University), Yongqiang Lv (Tsinghua University)

Adaptive Routing Algorithm for Joint Cloud Video Delivery
Towards Efficient Resource Management in Virtual Clouds
Bo An (Peking University), Junming Ma (Peking University), Donggang Cao (Peking University), Gang Huang (Peking University)

Monitoring and Billing of A Lightweight Cloud System Based on Linux Container
Yujian Zhu (Peking University), Junming Ma (Peking University), Bo An (Peking University), Donggang Cao (Peking University)

Building emulation framework for non-volatile memory
Guoliang Zhu (National University of Defense Technology), Kai Lu (National University of Defense Technology), Xiaoping Wang (National University of Defense Technology)

Seflow: Efficient Flow Scheduling for Data-Parallel Jobs
Qiao Zhou (National Lab for Parallel and Distributed Processing), Ziyang Li (National Lab for Parallel and Distributed Processing), Ping Zhong (Central South University), Tian Tian (National Lab for Parallel and Distributed Processing), Yuxing Peng (National Lab for Parallel and Distributed Processing)

Online Encoding for Erasure-Coded Distributed Storage Systems
Fangliang Xu (National University of Defense Technology), Yijie Wang (National University of Defense Technology), Xingkong Ma (National University of Defense Technology)

Accelerating Big Data Infrastructure and Applications
Kevin Brown (Tokyo Institute of Technology), Tianqi Xu (Tokyo Institute of Technology), Keita Iwabuchi (Tokyo Institute of Technology), Kento Sato (Lawrence Livermore National Laboratory), Adam Moody (Lawrence Livermore National Laboratory), Kathryn Mohror (Lawrence Livermore National Laboratory), Nikhil Jain (Lawrence Livermore National Laboratory), Abhinav Bhatle (Lawrence Livermore National Laboratory), Martin Schulz (Lawrence Livermore National Laboratory), Roger Pearce (Lawrence Livermore National Laboratory), Maya Gokhale (Lawrence Livermore National Laboratory), Satoshi Matsuoka (Tokyo Institute of Technology)

Disaster Network Evolution Using Dynamic Clustering of Twitter Data
Krishna Kant (Temple University), Yilang Wu (Aizu University), Shanshan Zhang (Temple University), Junbo Wang (Aizu University), Amitangshu Pal (Temple University)

Single-epoch supernova classification with deep convolutional neural networks
Akisato Kimura (NTT), Ichiro Takahashi (Kavli IPMU, The University of Tokyo), Masaomi Tanaka (National Astronomical Observatory of Japan), Naoki Yasuda (Kavli IPMU, The University of Tokyo), Naonori Ueda (NTT), Naoki Yoshida (Kavli IPMU, The University of Tokyo)

Enabling Large Scale Deliberation using Ideation and Negotiation-Support Agents
Katsuhide Fujita (Tokyo University of Agriculture and Technology), Takayuki Ito (Nagoya Institute of Technology), Mark Klein (MIT)

12:00-13:30 Monday, June 5, 2017
Lunch
Location: Savannah

13:30-15:30 Monday, June 5, 2017
Workshop: CCN-CPS, Session 3
Location: Salon II

Session Chair: Uttam Ghosh (Tennessee State University)

Optimal Deployment of Charging Stations for Electric Vehicles: A Formal Approach
Amarjit Datta (Tennessee Technological University), Brian Ledbetter (Tennessee Technological University), Mohammad Ashiqur Rahman (Tennessee Technological University)

Formal Verification of Control Strategies for a Cyber Physical System
Amjad Gawanmeh (Khalifa University of Science and Technology), Ali Alwadi (Auckland University of Technology), Sazia Parvin (University of New South Wales)

Lightweight Detection and Isolation of Black Hole Attacks in Connected Vehicles
Sami Albouq (Oakland University), Erik Fredericks (Oakland University)

A new threat assessment method for integrating an IoT infrastructure in an information system
Workshop: ADSN, Session 3: Network Assurance

Faulty Sensor Data Detection in Wireless Sensor Networks Using Logistical Regression
Tianyu Zhang (University of Hyogo), Qian Zhao (University of Hyogo), Yukikazu Nakamoto (University of Hyogo)

An Adaptability-Enhanced Routing Method for Multiple Gateway-based Wireless Sensor Networks Using Secure Dispersed Data Transfer
Ryuma Tani (Hiroshima City University), Kento Aoi (Hiroshima City University), Eitaro Kohno (Hiroshima City University), Yoshiaki Kakuda (Hiroshima City University)

Progressive Download Method Based on Timer-Driven Requesting Schemes Using Multiple TCP Flows on Multiple Paths
Hiroaki Horiba (Hiroshima City University), Tokumasa Hiraoka (Hiroshima City University), Junichi Funasaka (Hiroshima City University)

Workshop: PED-BGP, Session 1

Location: Salon VI

Keynote speech: Application-aware data dissemination
Bettina Kemme (McGill University)

WED-SQL: A Relational Framework for Design and Implementation of Process-Aware Information Systems
Bruno Padilha (University of Sao Paulo), André Luis Schwerz (Federal University of Technology), Rafael Liberato Roberto (Federal University of Technology)

Querying Workflow Logs
Yan Tang (University of California at Santa Barbara), Jianwen Su (University of California at Santa Barbara)

On the integration of event-based and transaction-based architectures for Supply Chains
Zhijie Li (Indiana University–Purdue University Indianapolis), Haoyan Wu (Indiana University–Purdue University Indianapolis), Brian King (Indiana University–Purdue University Indianapolis), Zina Ben-Miled (Indiana University–Purdue University Indianapolis), John Wassick (The Dow Chemical Company), Jeffrey Tazelar (The Dow Chemical Company)

Workshop: IoTCA, Session 1

Location: Atlanta

Keynote Speech: The Internet of Things, People, and Systems: From the Edge to the Cloud
Schahram Dustdar (TU Vienna)

Towards Privacy-Aware Smart Buildings: Capturing, Communicating, and Enforcing Privacy Policies and Preferences
Primal Pappachan (University of California Irvine), Martin Degelingly (Carnegie Mellon University), Roberto Yus (University of California Irvine), Anupam Dasy (Carnegie Mellon University), Sruti Bhagavatulay (Carnegie Mellon University), William Melichery (Carnegie Mellon University), Pardis Emami Naeini (Carnegie Mellon University), Shikun Zhang (Carnegie Mellon University), Lujo Bauery (Carnegie Mellon University), Alfred Kobsa (University of California Irvine), Sharad Mehrotra (University of California Irvine), Norman Sadeh (Carnegie Mellon University), Nalini Venkatasubramanian (University of California Irvine)

Deploying Data-Driven Security Solutions on Resource-Constrained Wearable IoT System
Hang Cai (Worcester Polytechnic Institute), Tianlong Yun (Worcester Polytechnic Institute), Josiah Hester (Dartmouth College), Krishna K. Venkatasubramanian (Clemson University)

A Motif based IoT Framework for Data Efficiency
Akash Sahoo (Texas A&M University), Rabi Mahapatra (Texas A&M University)

Workshop: WoSC, Session 1

Location: Columbia

Keynote Speech: Serverless Computing: Patterns and Road Ahead
Roger Barga (Amazon Web Services)

Ripple: Home Automation for Research Data Management
Ryan Chard (Argonne National Laboratory), Kyle Chard (Computation Institute, University of Chicago and Argonne National Lab), Jason Alt (National Center for Supercomputing Applications), Dilworth Parkinson (Lawrence Berkeley National Laboratory), Steve Tuecke (Computation Institute, University of Chicago and Argonne National Lab), Ian Foster (Argonne National Laboratory & The University of Chicago)
### Pipsqueak: Lean Lambdas with Large Libraries
Edward Oakes (University of Wisconsin-Madison), Leon Yang (University of Wisconsin-Madison), Kevin Houck (University of Wisconsin-Madison), Tyler Harter (Microsoft Gray Systems Lab), Andrea C. Arpaci-Dusseau (University of Wisconsin-Madison), Remzi H. Arpaci-Dusseau (University of Wisconsin-Madison)

### Leveraging the Serverless Architecture for Securing Linux Containers
Nilton Bila (IBM), Paolo Dettori (IBM), Ali Kanso (IBM), Yuji Watanabe (IBM), Alaa Youssef (IBM)

<table>
<thead>
<tr>
<th>Workshop: NSF-JST</th>
<th>Location: Savannah</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>15:30-16:00 Monday, June 5, 2017</strong></td>
<td></td>
</tr>
<tr>
<td>Coffee Break</td>
<td>Location: Foyer</td>
</tr>
<tr>
<td><strong>16:00-17:00 Monday, June 5, 2017</strong></td>
<td></td>
</tr>
<tr>
<td>Workshop: CCN-CPS, Session 4</td>
<td>Location: Salon II</td>
</tr>
<tr>
<td>Session Chair: Bruno Dorsemaine (Orange Labs)</td>
<td></td>
</tr>
<tr>
<td>A Security Framework for SDN-enabled Smart Power Grids</td>
<td>Uttam Ghosh (Tennessee State University), Pushpita Chatterjee (SRM RESEARCH INSTITUTE), Sachin Shetty (Old Dominion University)</td>
</tr>
<tr>
<td>Real-time Monitoring Steam Generators using a Hybrid Imaging System</td>
<td>Mahmoud Meribout (Petroleum Institute), Imran Saied (Petroleum Institute), Esra Al Hosani (Adco Group)</td>
</tr>
<tr>
<td>Securing big Data Efficiently through Microaggregation Technique and Huffman Compression</td>
<td>Shakila Mahjabin Torni (Bangladesh Army International University of Science and Technology), Mohammad Zahidur Rahman (Jahangirnagar University), Sazia Parvin (University of New South Wales), Amjad Gawannem (Khalifa University of Science and Technology)</td>
</tr>
<tr>
<td>Model Based Energy Consumption Analysis of Wireless Cyber Physical Systems</td>
<td>Jing Liu (Peking University), Ping Wang (Peking University), Jinlong Lin (Peking University), Chao-Hsien Chu (Pennsylvania State University)</td>
</tr>
<tr>
<td>Workshop: ADSN, Session 4: Panel on “Assurance in Internet of Things (IoT)”</td>
<td>Location: Salon IV</td>
</tr>
<tr>
<td>Moderator: Eitaro Kohno</td>
<td></td>
</tr>
<tr>
<td>Workshop: PED-BGP, Session 2</td>
<td>Location: Salon VI</td>
</tr>
<tr>
<td>CacheDOCS: A Dynamic Key-Value Object Caching Service</td>
<td>Julien Gascon-Samson (University of British Columbia), Michael Coppinger (McGill University), Fan Jin (McGill University), Jörg Kienzle (McGill University), Bettina Kemme (McGill University)</td>
</tr>
<tr>
<td>WolfPath: Accelerating iterative traversing-based graph processing algorithms on GPU</td>
<td>Huanzhou Zhu (University of Warwick), Ligang He (University of Warwick)</td>
</tr>
<tr>
<td>A Novel Auction-based Query Pricing Schema</td>
<td>Xingwang Wang (Jilin University), Xiaohui Wei (Jilin University), Shang Gao (Jilin University), Yuanyuan Liu (Jilin University), Zongpeng Li (University of Calgary)</td>
</tr>
<tr>
<td>BlockGraphChi: Enabling Block Update in Out-of-core Graph Processing</td>
<td>Zhiyuan Shao (Huazhong University of Science and Technology), Zhenjie Mei (Huazhong University of Science and Technology), Xiaofeng Ding (Huazhong University of Science and Technology), Hai Jin (Huazhong University of Science and Technology)</td>
</tr>
<tr>
<td>Workshop: IoTCA, Session 2</td>
<td>Location: Atlanta</td>
</tr>
<tr>
<td>CoTWare: A Cloud of Things Middleware</td>
<td>Jameela Al-Jaroodi (Robert Morris University), Nader Mohamed (Middleware Technologies Lab.), Imad Jawhar (Midcomp Research Center)</td>
</tr>
<tr>
<td>Securing the Internet of Things: A Meta-Study of Challenges, Approaches, and Open Problems</td>
<td></td>
</tr>
</tbody>
</table>
Mahmud Hossain (University of Alabama at Birmingham), Ragib Hasan (University of Alabama at Birmingham), Anthony Skjellum (Auburn University)

Internet of Things Framework for Smart Learning Analytics
Ali Yavari (Swinburne University of Technology), Reza Soltanpoor (RMIT University)

**Workshop: WoSC, Session 2**
**Location: Columbia**

Serverless Computing: Design, Implementation, and Performance
Garrett McGrath (University of Notre Dame), Paul R. Brenner (University of Notre Dame)

Panel debate on the novelty and challenges of serverless computing
Participants: TBA

**Workshop: NSF-JST**
**Location: Savannah**

**17:00-18:00 Monday, June 5, 2017**

Workshop: PED-BGP, Session 2
**Location: Salon VI**

Incremental Parallel Computing using Transactional Model in Large-scale Dynamic Graph Structures
Anand Tripathi (University of Minnesota), Rahul R. Sharma (University of Minnesota), Manu Khandelwal (University of Minnesota), Tanmay Mehta (University of Minnesota), Varun Pandey (University of Minnesota)

Against Signed-Graph Deanonymization Attacks: Privacy Protection for Social Networks
Jianliang Gao (Central South University), Yu Liu (Central South University), Ping Zhong (Central South University), Jianxin Wang (Central South University)
Understanding and Improving Temporal Fairness on an Electronic Trading Venue
Hayden Melton (Deakin University)

Fairness, in general, is a topic that has received much attention in research on distributed systems. In their application as electronic trading venues, however, temporal fairness remains a topic that is poorly understood. This is concerning because operators of these venues generally have obligations to ensure their fairness. Consequently, this paper (1) describes what temporal fairness is and is not, (2) identifies things that can make it elusive, and (3) describes a mechanism for improving it that was recently retrofitted to a major FX trading venue: Thomson Reuters Matching.

CertificateLess Cryptography-based Rule Management Protocol for Advanced Mission Delivery Networks
Jongho Won (Purdue University), Ankush Singla (Purdue University), Elisa Bertino (Purdue University)

Assured Mission Delivery Network (AMDN) is a collaborative network to support data-intensive scientific collaborations in a multi-cloud environment. Each scientific collaboration group, called a mission, specifies a set of rules to handle computing and network resources. Security is an integral part of the AMDN design since the rules must be set by authorized users and the data generated by each mission may be privacy-sensitive. In this paper, we propose a CertificateLess cryptography-based Rule-management Protocol (CL-RP) for AMDN, which supports authenticated rule registrations and updates with non-repudiation. We evaluate CL-RP through test-bed experiments and compare it with other standard protocols.

Faulty Sensor Data Detection in Wireless Sensor Networks Using Logistical Regression
Tianyu Zhang (University of Hyogo), Qian Zhao (University of Hyogo), Yukikazu Nakamoto (University of Hyogo)

Wireless sensor networks (WSNs) are commonly used to monitor changes in an environment and prevent disasters such as structural instability, forest fires, and tsunamis. WSNs should rapidly respond to changes and must process and analyze sensor data in a distributed way to minimize battery consumption. On the other hand, machine learning (ML) algorithms are a powerful tool for data analyzing. However, ML algorithms are so complex that cannot be executed on resource constrained sensor nodes. Another challenge of using ML algorithms in WSNs is that ML algorithms are difficult to be distributed on every sensor node. Because ML algorithms are based on statistics’ methods that need collecting amount of data to approach accuracy. In this paper, we propose a method that divides a logistical regression ML method into two steps, then distributes the two steps onto sink node and sensor nodes to detect faulty sensor data.

An Adaptability-Enhanced Routing Method for Multiple Gateway-based Wireless Sensor Networks Using Secure Dispersed Data Transfer
Ryuma Tani (Hiroshima City University), Kento Aoi (Hiroshima City University), Eitaro Kohno (Hiroshima City University), Yoshiaki Kakuda (Hiroshima City University)

In conventional wireless sensor networks (hereinafter referred to as WSNs), the single sink node model has been employed to collect and store the measured data to provide to the external users of WSNs. However, the single sink model of WSNs can be the single point of failure for some usage. To counter this problem, we can employ multiple gateway-based WSNs. In addition, WSNs are susceptible to various kinds of attacks such as eavesdropping. To counter eavesdropping, we already have proposed the secret sharing scheme-based secure dispersed data transfer method (hereinafter referred to as the secure dispersed data transfer method). While we had confirmed that the secure dispersed data transfer method is effective to counter eavesdropping through the use of radio area disjoint multiple paths, we also found that the secure dispersed data transfer method cannot be effective in severe environments such as in a network with a low density of nodes.

A Progressive Download Method Based on Timer-Driven Requesting Schemes Using Multiple TCP Flows on Multiple Paths
Hiroaki Horiba (Hiroshima City University), Tokumasa Hiraoka (Hiroshima City University), Junichi Funasaka (Hiroshima City University)

Due to the widespread use of broadband communication media, the conventional TCP cannot fully utilize such broad bandwidth, so many improvements on TCP itself and a lot of accelerating methods which use multiple TCP flows have been proposed. In addition, video hosting services on the Internet as a new medium have become popular, and progressive downloading methods, which download segmented video data while relaying them, are adopted on various sites. The playback quality of progressive download methods has been improved by the existing method which establishes multiple TCP flows on each of multiple paths. However, the existing method assumes that bandwidth, delay, and packet loss rate of each path are known. Therefore, in this paper, a method using the timer-driven requesting scheme which is to be effective even when bandwidth, delay, and packet loss rate are not given. Moreover, it features duplicate requesting scheme to cope with quality deterioration in video playback due to out-of-order block arrivals when applying progressive download using multiple paths. This paper evaluates the proposed method comparing with the existing method by simulation. As a result, it is found that the proposed method yields high performance enough to keep the video quality higher than the existing method even though the network condition is not clarified in advance. The proposal can be regarded as an assurance network technology since it can adapt to the current network status and keep the playback rate high.
WolfPath: Accelerating iterative traversing-based graph processing algorithms on GPU
Huanzhou Zhu (University of Warwick), Ligang He (University of Warwick)

There is the significant interest nowadays in developing the frameworks for parallelizing the processing for the large graphs such as social networks, web graphs, etc. Most parallel graph processing frameworks employ iterative processing model. However, by benchmarking the state-of-art GPU-based graph processing frameworks, we observed that the performance of iterative traversing-based graph algorithms (such as Bread First Search, Single Source Shortest Path and so on) on GPU is limited by the frequent data exchange between host and GPU. In order to tackle the problem, we develop a GPU-based graph framework called WolfPath to accelerate the processing of iterative traversing-based graph processing algorithms. In WolfPath, the iterative process is guided by the graph diameter to eliminate the frequent data exchange between host and GPU. To accomplish this goal, WolfPath proposes a data structure called Layered Edge list to represent the graph, from which the graph diameter is known before the start of graph processing. In order to enhance the applicability of our WolfPath framework, a graph preprocessing algorithm is also developed in this work to convert any graph into the format of the Layered Edge list. We conducted extensive experiments to verify the effectiveness of WolfPath. The experimental results show that WolfPath achieves significant speedup over the state-of-art GPU-based in-memory and out-of-memory graph processing frameworks.

A Novel Auction-based Query Pricing Schema
Xingwang Wang (Jilin University), Xiaohui Wei (Jilin University), Shang Gao (Jilin University), Yuanyuan Liu (Jilin University), Zongpeng Li (University of Calgary)

As a common processing method, query is widely used in many areas, such as graph processing, machine learning, statistics, etc. However, queries are usually priced according to vendor-specified fixed views (API) or number of transactions, which ignores the heterogeneity of queries (computing resource consumption for query and information that the answer brings) and violates the monotone principle.

In this work we study the relational query pricing problem by taking both information (i.e., data) value and query resource consumptions into account. We design efficient auctions for query pricing. Different from the existing query pricing schemas, query auction determines data prices that reflect the demand-supply of shared computing resources and information value (i.e., price discovery). We target query auction that runs in polynomial time and achieves near-optimal social welfare with a good approximation ratio, while elicits truthful bids from consumers. Towards these goals, we adapt the posted pricing framework in game-theoretic perspective by casting the query auction design into an Integer Linear Programming problem, and design a primal-dual algorithm to approximate the NP-hard optimization problem. Theoretical analysis and empirical studies driven by real-world data market benchmark verify the efficiency of our query auction schema.

BlockGraphChi: Enabling Block Update in Out-of-core Graph Processing
Zhiyuan Shao (Huazhong University of Science and Technology), Zhenjie Mei (Huazhong University of Science and Technology), Xiaofeng Ding (Huazhong University of Science and Technology), Hai Jin (Huazhong University of Science and Technology)

In the past several years, lots of out-of-core graph processing systems are built to process big graph datasets in computer systems with limited memory. Due to the iterative nature of graph algorithms, most of these systems employ synchronous execution model to organize the computation, i.e., divide the computing into multiple rounds, each of which corresponds to one iteration of the graph algorithm. In order to fully utilize the disk bandwidth, these systems sequentially scan the whole graph dataset at each iteration. However, as the graph dataset under processing may be huge, more iterations generally means larger I/O overheads. Although asynchronous implementation of the synchronous execution model allows message passing within an iteration, the effectiveness is still limited. Since in such model, at most one message is allowed to be passed from one vertex to another.

In this paper, we investigate the idea of block updating in the synchronous execution model framework in the out-of-core graph processing systems. With this new model, the system conducts graph algorithm on the loaded subgraph (i.e., block) to its local convergence, and then switches to other subgraphs to continue this process, until the global convergence is reached. We implement this new model in GraphChi (the result system is called BlockGraphChi), and propose a graph partition method, named as DMUP, to cooperate with this new model. By this study, we found that compared with the original execution model of GraphChi: 1) the new model can generally reduce the amount of iterations (and thus the I/O overheads) for graph algorithms, while the extent of reduction depends on the method of graph partitioning and the properties of the algorithms; 2) the new model can dramatically reduce the overall execution time of graph traversal algorithms (by up to 31.4x), and better partitioning method leads to better performance; 3) the new model has much smaller effectiveness on improving the overall performance of fix-point algorithms, such as PageRank, due to the increased computational overhead.

Incremental Parallel Computing using Transactional Model in Large-scale Dynamic Graph Structures
Anand Tripathi (University of Minnesota, Minneapolis), Rahul R. Sharma (University of Minnesota), Manu Khandelwal (University of Minnesota), Tanmay Mehta (University of Minnesota), Varun Pandey (University of Minnesota)

Many graph analytics problems benefits from the use of parallel computing techniques to reduce the execution time, which can still be quite high for large graph problems. The goal of our work is to eliminate the need of re-executing an analytics program when the graph structure is modified with a small set of updates after the initial execution of the program. Towards this goal, we present here the results of our investigation of incremental computation techniques in dynamic graph
structures using a transactional model of parallel programming. In this model, computation tasks in an analytics application are executed in parallel as serializable transactions. This paper describes how incremental computation techniques are supported by this model for dynamic graph structures. We use the problems of finding connected-components in a graph and the graph coloring problem to illustrate our approach for incremental computations. Using experimental evaluations, we show the benefits of this approach.

**Against Signed-Graph Deanonymization Attacks: Privacy Protection for Social Networks**

Jianliang Gao (Central South University), Yu Liu (Central South University), Ping Zhong (Central South University), Jianxin Wang (Central South University)

Social networks are usually presented as graphs. But the topological characteristics of graphs could be used by attackers to deanonymize target entities in social networks. Existing works mostly have an assumption that attacker knows only the target entities’ neighborhood graph. This assumption might result in privacy leakage because of the ignorance of link property between entities. In real applications, attackers might re-identify entities in social networks based on not only the links between entities, but also the property of links. In this paper, we take the property of links into consideration for the first time when achieving $k$-anonymity for social networks, which means the attackers cannot re-identify a target with confidence higher than $1/k$. The links are cataloged as positive and negative, which is called signed graph. In this background, we propose a $k$S-anonymization scheme to protect the privacy of key entities in social networks. The proposed scheme minimizes the amount of modification on original graphs, which preserves the utility of the original data. Extensive experiments on real data sets and synthetic graph illustrate the effectiveness of the proposed scheme. The utility of anonymized networks are remained by demonstrating with the results of vertex degree, betweenness, closeness and their Kolmogorov-Smirnov (K-S) test.
Policies Guiding Cohesive Interactions among Internet of Things with Communication Cloud and Social Networks
Henry Hexmoor (Southern Illinois University)

Cohesive interaction among Internet of thing nodes will benefit from formation of ad hoc communication network clouds for rapid exchange of information that is pertinent for their successful interaction. Long enduring interactions among such nodes will benefit from ad hoc socially linked networks for collaboration on shared objectives. We present guidelines for forming and using these constructs and policies that constrain them to requirements of specific applications.

Enhanced Security of Building Automation Systems Through Microkernel-Based Controller Platforms
Xiaolong Wang (University of South Florida), Richard Habeeb (University of South Florida), Xinming Ou (University of South Florida), Siddharth Amaravadi (Kansas State University), John Hatclif (Kansas State University), Masaaki Mizuno (Kansas State University), Mitchell L Neilsen (Kansas State University), Raj Rajagopalan (Honeywell), Srivatsan Varadarajan (Honeywell Aerospace Advanced Technology Labs)

A Building Automation System (BAS) is a complex distributed Cyber-Physical System that controls building functionalities such as heating, ventilation, and air condition-ing (HVAC), lighting, access, emergency control, and so on. There is a growing opportunity and motivation for BAS to be integrated into enterprise IT networks together with various new “smart” technologies to improve occupant comfort and reduce energy consumption. These new technologies coexist with legacy applications, creating a mixed-criticality environment. In this environment, as systems are integrated into IT networks, new attack vectors are introduced. Thus, networked non-critical applications running on the OS platform may be compromised, leaving the control systems vulnerable. The industry needs a reliable computing foundation that can protect and isolate these endangered critical systems from untrusted applications.

This work presents a novel kernel-based approach to secure critical applications. Our method uses a security-enhanced, microkernel architecture to ensure the security and safety properties of BAS in a potentially hostile cyber environment. We compare three system design and implementations for a simple BAS scenario: 1) using the microkernel MINIX 3 enhanced with mandatory access control for inter-process communication (IPC), 2) using sel4, a formally verified, capability-based microkernel, and 3) using Linux, a monolithic kernel OS. We show through experiment that when the non-critical applications are compromised in both MINIX 3 and sel4, the critical processes that impact the physical world are not affected. Whereas in Linux, the compromised applications can easily disrupt the physical processes, jeopardizing the safety properties in the physical world. This shows that microkernels are a superior platform for BAS or other similar control environments from a security point of view, and demonstrates through example how to leverage the architecture to build a robust and resilient system for BAS.

High Level Design of a Home Autonomous System Based on Cyber Physical System Modeling
Basman Alhafidh (Florida Institute of Technology), William H. Allen (Florida Institute of Technology)

The process used to build an autonomous smart home system using cyber-physical systems (CPS) principles has received much attention by researchers and developers. However, there are many challenges during the design and implementation of such a system, such as Portability, Timing, Prediction, and Integrity. This paper presents a novel modeling methodology for a smart home system in the scope of cyber-physical interface that attempts to overcome these issues. We discuss a high-level design approach that simulates the first three levels of a SC architecture in CPS layers in a smart home environment. A detailed description of the model design, architecture, and a software implementation via NetLogo simulation program will be presented. Our design provides an example for developers on how to implement an ecosystem in a home environment as part of a smart cities’ infrastructure based on CPS design principles.

A Cyber Physical Buses-and-Drones Mobile Edge Infrastructure for Large Scale Disaster Emergency Communications
Mamta Narang (Auckland University of Technology), William Liu (Auckland University of Technology), Jairo A Gutierrez (Auckland University of Technology), Luca Chiaraviglio (University of Rome Tor Vergata)

Immediately after a disaster, the normal telecommunication infrastructure, including wired and wireless networks, is often seriously compromised and cannot guarantee regular coverage and reliable communications services. These temporarily-missing communications capabilities are crucial to rescuers and affected citizens as the responders need to effectively coordinate and communicate to minimize the loss of lives and property. A cyber-physical system (CPS) is composed of integrated communication, computation and physical objects, and cyber-physical vehicle systems (CPVVs) are an emerging field due to the rapid advancements on real-time computing, mobile communications and autonomous control in intelligent transport systems. In this paper, we propose a cyber-physical buses-and-drones mobile edge infrastructure (AidLife) for disaster emergency communications, which aims at a rapidly deployable resilient system capable of supporting flexible communications to serve large-scale disaster situations by utilizing the existing public transport system. In particular we envision a proposal where public buses can be recruited to temporarily host portable base station (BS) and computation units as well as power resources so as to form a buses-based mobile edge infrastructure, and also accommodate drones to extend their coverage to hard-to-reach areas. Our preliminary results show that the AidLife system can guarantee a good coverage to users, even when a large number of normal BSs that are damaged.

A Performance Comparison of Containers and Virtual Machines in Workload Migration Context
Kumar Gaurav (VMware Software India Pvt Ltd), Pavan Karkun (VMware Software India Pvt LTD), Y. C. Tay (National University of Singapore)

This paper gives a mathematical framework for decision making around placing and migrating workloads in a data-center where applications are packaged as OS containers running on virtual machines. The decision point on VM migration vs container kill/restart, VM fork vs container spawn are studied here. We propose a mathematical model for the migration of workloads aforementioned cases and also for shared memory decay in case of forking a virtual machine. Experimental results are analyzed to determine the validity of the model.

Towards Service-Oriented Middleware for Cyber Physical Systems
Nader Mohamed (Middleware Technologies Lab.), Sanja Lazarova-Molnar (University of Southern Denmark)

Cyber-Physical Systems (CPS) provide many smart features for enhancing physical systems and environments. They are designed with a set of distributed hardware, software, and network components that are embedded in physical systems and environments or attached to humans. Many CPS at different scales are being developed for a variety of applications that provide valuable interactions between the cyber world and the physical systems and environments. However, these developments face many challenges due to the complexity of these applications. An appropriate middleware is needed to provide infrastructural support and assist
the development and operations of diverse CPS applications. This paper studies utilizing the service-oriented middleware approach for CPS and discusses the advantages and requirements for such utilization. In addition, it proposes a service-oriented middleware for CPS, called CPSWare. This middleware views all CPS components as a set of services and provides an infrastructure to develop and operate CPS applications. This approach provides systemic solutions for solving many computing and networking issues in CPS. It also enables the integration of CPS with other systems such as Cloud Computing and Fog Computing. In addition, as CPS can be developed for various applications at different scales, this paper provides a classification for CPS applications and discusses how CPSWare can effectively deal with these categories.

**Networking and Communication in Cyber Physical Systems**

Imad Jawhar (UAE University), Jameela Al-Jaroodi (Robert Morris University)

Cyber-physical systems (CPSs) are emerging as a new technology, which is used to provide seamless interaction between the physical and cyber worlds. This novel paradigm is a natural evolution and extension of wireless sensor networks (WSNs) and control models to allow for effective monitoring and control of physical systems from the computing environment. In order to support this interface and allow such smooth interactions, efficient networking and communication between the physical and cyber worlds take a very important and critical role. In this paper, we identify the various applications and categories of CPS systems, and characterize the associated data traffic that is generated. We also discuss the different protocols and requirements that are needed at the various networking layers for these applications. Subsequently, we identify important parameters such as bandwidth, delay, reliability, security, and mobility, which are essential in order to allow for effective and robust operation of the various CPS systems.

**Optimal Deployment of Charging Stations for Electric Vehicles: A Formal Approach**

Amarjit Datta (Tennessee Technological University), Brian Ledbetter (Tennessee Technological University), Mohammad Ashiqur Rahman (Tennessee Technological University)

Electric vehicles (EVs) are a fascinating innovation of the modern automobile industry. Due to their attractive features and a growing worldwide environmental awareness, the number of EV purchases is growing at an increasing rate day by day. As the price of EVs is expected to drop in the near future, a large number of new EVs will hit the road consequently. However, our current infrastructure is not capable of supporting this growing number of EVs. We need more charging stations, placed optimally across an area, each equipped with multiple charging outlets to charge the incoming EVs in a reasonable amount of time. In this paper, we present a formal framework to optimally deploy charging stations for EVs in a given area. The framework designs this verification as an optimization problem where the goal is to optimally place the charging stations with a sufficient number of charging outlets to serve all EVs in a given area while satisfying the limited budget and other system constraints. We evaluate the proposed framework for its analysis capability as well as its scalability by executing experiments on different synthetic test cases.

**Formal Verification of Control Strategies for a Cyber Physical System**

Ajmal Gawanmeh (Khalifa University of Science and Technology), Ali Alwadi (Auckland University of Technology), Sazia Parvin (University of New South Wales)

Cyber Physical Systems (CPS) use emerging computing, communication, and control methods to monitor and control geographically dispersed critical system components to allow a high level of confidence about their operation. Simulation methods are frequently used in testing such critical system components, however, it might not be adequate to show the absence of errors given the complexity of the system components under test. Failure in detecting errors in safety critical systems can lead to a catastrophic situation. In this paper, we propose an approach, based on simulation and formal analysis, for the reliability analysis of CPS. We illustrate this approach on an industrial case study that demonstrates several challenging features in the design and implementation of CPS. Experimental results obtained show that the proposed approach is efficiently used in order to test and verify the four tanks process system, where simulation results show the validity of approximation and abstraction of the system, and formal analysis is used to validate that several design requirements were satisfied in the control strategies proposed.

**Lightweight Detection and Isolation of Black Hole Attacks in Connected Vehicles**

Sami Albuq (Oakland University), Erik Fredericks (Oakland University)

Connected Vehicles (CVs) can be exposed to black hole attacks that deceive legitimate nodes by falsifying an attractive route to a destination node. This occurs when an attacker sends a packet to the source node confirming the existence of a fresh route. In this paper, we propose a Black Hole Detection Protocol (BlackDP) that works on a highway divided into clusters and monitored by Road Side Units (RSUs) to detect both single and cooperative black hole attacks. Every RSU is tasked with performing both detection and isolation of black hole attacks for their respective highway section after authentication violations and suspicious route establishment activities that have been reported by a legitimate node. The design goal of BlackDP is to decouple the detection process from mobile nodes and construct a trusted semi-centric detection process that can collect needed information for lightweight detection and reliable isolation of malicious nodes. We validate BlackDP in a simulated highway environment to demonstrate its effectiveness.

**A new threat assessment method for integrating an IoT infrastructure in an information system**

Bruno Dorsemaine (Orange Labs), Jean-Philippe Gaujot (Orange Labs), Jean-Philippe Wary (Orange Labs), Nizar Kheir (Thales), Pascal Urien (Telecom ParisTech)

In this paper, we propose a new approach to manage the threats brought by an IoT infrastructure to an information system (IS). We first give a state of art for information security properties in IoT and IS based on standards such as ISO 16982 and ISO 27005 and a previously published taxonomy. Then we detail an innovative method, based on the evaluation of threats brought by an IoT infrastructure onto an IS. It is represented as a qualitative matrix between IoT infrastructure threats and the Security properties of the IS. The method is then applied to the use case of connected light bulbs. Thanks to this approach, it is possible to logically organize threat management while integrating an IoT infrastructure into an IS.

**A Security Framework for SDN-enabled Smart Power Grids**

Uttam Ghosh (Tennessee State University), Pushpita Chatterjee (SRM RESEARCH INSTITUTE), Sachin Shetty (Old Dominion University)

Emerging software defined networking (SDN) paradigm provides flexibility in controlling, managing, and dynamically reconfiguring smart grid networks. It can be seen in the literature that considerably less attention has been given to provide security in SDN-enabled smart grid networks. Most of the efforts focus on protecting
smart grid networks against various forms of outsider attacks only by providing consistent access control, applying efficient and effective security policies, and managing and controlling the network through the use of a centralized SDN controller. Furthermore, centralized SDN controllers are plagued by reliability and security issues. This paper presents a framework with multiple SDN controllers and security controllers that provides a secure and robust smart grid architecture. The proposed framework deploys a local IDS in a substation to collect the measurement data periodically and to monitor the control-commands that are executed on SCADA slaves. A global IDS in control center collects the measurement data from the substations and estimates the state of the smart grid system by utilizing the theory of differential evolution. The global IDS further verifies the consequences of control-commands issued by SDN controller and SCADA master. An alarm is generated upon detection of an attacker or unsteady state of the smart grid system. The framework also deploys light-weight identity based cryptography to protect the smart grid network from outside attacks. Performance comparison and initial simulation result have been presented to show that the proposed framework is effective as compared to existing security frameworks for SDN-enabled smart grids.

Real-time Monitoring Steam Generators using a Hybrid Imaging System
Mahmoud Meribout (Petroleum Institute), Imran Saied (Petroleum Institute), Esra Al Hosani (Adco Group)
This paper presents a hybrid device for real-time measurement and imaging of solid and liquid contaminants that may occur in steam generators. The device uses a dedicated Near Infrared-Red device to determine the type of contaminants (i.e. water droplets and iron oxide particles) and a THz imaging system which measures the amount of contaminants as well as its flow rate. The NIR device can also determine the concentration of contaminants at sub-ng accuracy when its value is relatively low using spectrometry technique combined with principal component analysis (PCA). Three principal components (PC1, PC2, and PC3) were enough for this purpose. The PCA classification was performed using the least square support vector machine (LS-SVM) method. In case of relatively high concentration, the THz imaging system which uses block-based motion estimation algorithm can determine the velocity of individual contaminant particles to compute the global motion vector, the intensity and direction of which represents the overall flow rate and flow regime of the contaminants. The usage of image processing techniques together with NIR spectrometry constitutes a new promising step in flow metering. This is demonstrated by the extensive experiments which have been conducted for different scenario where the NIR subsystem system could determine the concentration of water droplets and solid contaminants with a maximum uncertainty of +/- 1.45% and +/- 1.16% respectively. With the NIR subsystem, pixel-level accuracy of motion vector was achieved, while the concentration of solid contaminants showed consisted proportionality with the average pixel intensity.

Securing big Data Efficiently through Microaggregation Technique and Huffman Compression
Shakila Mahjabin Tonni (Bangladesh Army International University of Science and Technology), Mohammad Zahidur Rahman (Jahangirnagar University), Sazia Parvin (University of New South Wales), Amjad Gawannneh (Khalifa University of Science and Technology)
Cyber-Physical Systems (CPS) requires big data communications as well as integration from several distributed sources. This data can usually be interconnected with physical applications, such as power grids or SCADA systems. In addition, it can be publicly accessible for using by third party users or data scientists. Therefore, it becomes imperative to ensure that this big data is well secured. Microaggregation is an widely used technique to protect a dataset through anonymity in order to prevent exposure of a person’s identity. This data disclosure may also result from an unpredicted data linkage with another dataset. As, most of these survey datasets store records using numerical values, many of the microaggregation techniques are developed and tested on numerical data. These algorithms are not suitable for those data where both numerical and categorical data are stored. In this paper we're proposing a microaggregation technique in order to provide data anonymity regardless of its type. The records are clustered into several groups using an evolutionary attribute grouping algorithm and each group records are then microaggregated applying Huffman data compression algorithm.

Model Based Energy Consumption Analysis of Wireless Cyber Physical Systems
Jing Liu (Peking University), Ping Wang (Peking University), Jinlong Lin (Peking University), Chao-Hsien Chu (Pennsylvania State University)
Wireless mesh networks begin to be used as an infrastructure of cyber-physical systems. A critical issue in developing wireless cyber physical systems (WCPSs) is the limited amount of energy available in the nodes. Energy consumption analysis can help designer to conduct a power-aware design process. In this paper, we propose a model based energy consumption analysis framework at architecture level for WCPSs. We extract event chains from the architecture model, with the energy consumption model for processing each type of event, we can estimate the energy consumption for each control loop and each node, as well as the overall energy consumption. All these energy consumption indexes can help us to design a performance and energy consumption balanced WCPS.
Router-based Brokering for Surrogate Discovery in Edge Computing
Julien Gedeon (Technische Universität Darmstadt), Christian Meurisch (Technische Universität Darmstadt), Disha Bhat (Technische Universität Darmstadt), Michael Stein (Technische Universität Darmstadt), Lin Wang (Technische Universität Darmstadt), Max Mühlhäuser (Technische Universität Darmstadt)

In-network processing pushes computational capabilities closer to the edge of the network, enabling new kinds of location-aware, real-time applications, while preserving bandwidth in the core network. This is done by offloading computations to more powerful or energy-efficient surrogates that are opportunistically available at the network edge. In mobile and heterogeneous usage contexts, the question arises how a client can discover the most appropriate surrogate in the network for offloading a task. In this paper, we propose a brokering mechanism that matches a client with the best available surrogate, based on specified requirements and capabilities. The broker is implemented on standard home routers, and thus, leverages the ubiquity of such devices in urban environments. To motivate the feasibility of this approach, we conduct a coverage analysis based on collected access point locations in a major city. Furthermore, the brokering functionality introduces only a minimal resource overhead on the routers and can significantly reduce the latency compared to distant, cloud-based solutions.

Modeling the Spread of Influence for Independent Cascade Diffusion Process in Social Networks
Zesheng Chen (Indiana University - Purdue University Fort Wayne), Kurtis Taylor (Indiana University - Purdue University Fort Wayne)

Modeling the spread of influence in online social networks is important for predicting the influence of individuals and better understanding many scenarios in social networks, such as the influence maximization problem. The previous work on modeling the spread of influence makes the assumption that the statuses of nodes in a network are independent of each other, which is apparently not correct for social networks. The goal of this work is to derive an accurate mathematical model to characterize the spread of influence for the independent cascade diffusion process in online social networks. Specifically, we apply the susceptible-infected-recovered epidemic model from epidemiology to characterize the independent cascade diffusion process and derive a general mathematical framework. To approximate the complex spatial dependence among nodes in a network, we propose a Markov model to predict the spread of influence. Through the extensive simulation study over several generated topologies and a real coauthorship network, we show that our designed Markov model has much better performance than the existing independent model in predicting the influence of individuals in online social networks.

Thank You For Being A Friend: An Attacker View on Online-Social-Network-based Sybil Defenses
David Koll (University of Goettingen), Martin Schwarzmaier (University of Goettingen), Jun Li (University of Oregon), Xiang-Yang Li (University of Science and Technology of China), Xiaoming Fu (University of Goettingen)

Online Social Networks (OSNs) have become a rewarding target for attackers. One particularly popular attack is the Sybil attack, in which the adversary creates many fake accounts called Sysbils in order to, for instance, distribute spam or manipulate voting results. A first generation of defense systems tried to detect these Sybils by analyzing changes in the structure of the OSN graph—unfortunately with limited success. Based on these efforts a second generation of solutions enriches the graph-structural approaches with higher-level user features in order to detect Sybil nodes more efficiently. In this work we provide an in-depth analysis of these defenses. We describe their common design and working principles, analyze their vulnerabilities, and design simple yet effective attack strategies that an adversary could launch to circumvent these systems. In our evaluation we reveal that an miscreant can exploit the credulity of OSN users and follow a targeted attack strategy to successfully avoid detection by all existing approaches.

Efficient Dynamic Service Function Chain Combination of Network Function Virtualization
Wenke Yan (Beijing University of Posts and Telecommunications), Conghui Zhu (Beijing University of Posts and Telecommunications), Lin Zhang (Beijing University of Posts and Telecommunications), Sixi Su (Beijing University of Posts and Telecommunications)

Network Function Virtualization (NFV) and Software Defined Network (SDN) are recently introduced to provide the virtualization technology for tackling the deployment of network service functions in corporate networks, broadband access networks, and more recently in data centers. How to enhance the flexibility, efficiency and effective of service function deployment is full of challenge. Although Service Function Chain (SFC) is carried out to support the flexibility of network services, it still needs one step forward to fulfill the efficient and effective combination of network services. In this paper, we propose an orthogonal crossover differential evolution (OXDE) to optimize SFC combination with respect to processing delay, energy consumption, and packet loss rate. The evaluation results show that the proposed OXDE algorithm outperforms the other algorithms and it can achieve the efficiency and effectiveness of SFC combination.

When Augmented Reality meets Big Data
Carlos Bermejo (The Hong Kong University of Science and Technology), Zhanpeng Huang (The Hong Kong University of Science and Technology), Tristan Braud (The Hong Kong University of Science and Technology), Pan Hui (The Hong Kong University of Science and Technology)

We live in an era where we are overloaded with data, and this can be the key for gaining rich insights about our world. Augmented reality (AR) enables us the possibility to visualise and analyse the growing torrent of data in a interactive, usable canvas. We can display complex data structures in simpler and more understandable ways that was not possible before. Big Data is a new paradigm results from the myriad data sources such as transactions, Internet, social networks, health care devices and sensor networks. AR and big data have a logical maturity that inevitably will converge. The trend of harnessing AR and big data to breed new interesting applications is starting to have a tangible presence. In this paper, we explore the potential to capture value from the marriage between AR and big data technologies, following with several challenges that must be addressed to fully realize this potential.

Sampling Based Efficient Algorithm to Estimate the Spectral Radius of Large Graphs
Samar Abbas (Lahore University of Management Sciences), Juvaria Tariq (Lahore University of Management Sciences), Arif Zaman (Lahore University of Management Sciences), Imdadullah Khan (Lahore University of Management Sciences)

Evaluating an extremely useful graph property, the spectral radius (largest absolute eigenvalue of the graph adjacency matrix), for large graphs requires excessive computing resources. This problem becomes especially challenging, for instance with distributed or remote storage, when accessing the whole graph itself is expensive in terms of memory or bandwidth. One approach to tackle this challenge is to estimate the spectral radius of the graph while reading only a small portion
of the graph. In this paper we present a sampling approach to estimate the spectral radius of large graphs. We define a score for vertices that i) is more of a combinatorial nature and is easier to compute and ii) has solid theoretical justifications hence, it closely approximate a vertex's contribution to the largest eigenvalue of the graph. Using this score, we model the sampling problem as a budgeted optimization problem and design a greedy algorithm to select a subgraph whose spectral radius approaches that of the whole graph. We provide analytical bound on computational complexity of our algorithm. We demonstrate effectiveness of our algorithm on various synthetic and real-world graphs and show that our algorithm also empirically outperforms known techniques.

Furthermore, we compare the quality of our results to estimates obtained from well known upper and lower bounds known in the spectral graph theory literature.

**Extemporaneous Micro-Mobile Service Execution Without Code Sharing**
Zheng Song (Virginia Tech), Minh Le (Utah State University), Young-Woo Kwon (Utah State University), Eli Tilevich (Virginia Tech)

In mobile edge computing, a mobile or IoT device requests a nearby device to execute some functionality and return back the results. However, the executable code must either be pre-installed on the nearby device or be transferred from the requester device, reducing the utility or safety of device-to-device computing, respectively. To address this problem, we present a micro-service middleware that executes services on nearby mobile devices, with a trusted middleman distributing executable code. Our solution comprises (1) a trusted store of vetted mobile services, self-contained executable modules, downloaded to devices and invoked at runtime; and (2) a middleware system that matches service requirements to available devices to orchestrate the device-to-device communication. Our experiments show that our solution (1) enables executing mobile services on nearby devices, without requiring a device to receive executable code from an untrusted party; (2) supports mobile edge computing in practical settings, increasing performance and decreasing energy consumption; (3) reduces the mobile development workload by reusing services.

**Preventing Colluding Identity Clone Attacks in Online Social Networks**
Georges A. Kamhoua (Florida International University), Niki Pissinou (Florida International University), S.S. Iyengar (Florida International University), Jonathan Beltran (Florida International University), Charles Kamhoua (Air Force Research Laboratory), Brandon L Hernandez (UTRGV), Laurent Njilla (Air Force Research Laboratory)

Nowadays, Online Social Networks (OSNs) become one of the most common way amongst people to facilitate communication, this has made it a target for attackers to steal information from influential users. This has brought new forms of customized attacks for OSNs. Attackers take advantage of the user trustworthiness when using OSN. This exploitation leads to attacks with a combination of both classical and modern threats. Specifically, colluding attackers have been taken advantage of many OSNs by creating fake profiles of friends of the target in the same OSN or others. Colluders impersonate their victims and ask friend requests to the target in the aim to infiltrate her private circle to steal information. This type of attacks are difficult to detect in OSNs because multiple malicious users may have a similar purpose to gain information from their targeted user. In this paper, to overcome this type of attack, we first address the problem of matching user profiles across multiple OSNs; second, by using both textual and features extracted from user profile and based on supervised learning techniques, we build a classifier. Simulation and experimental results are provided to validate the accuracy of our findings.
Towards Privacy-Aware Smart Buildings: Capturing, Communicating, and Enforcing Privacy Policies and Preferences
Primal Pappas (University of California Irvine), Martin Degeling (Carnegie Mellon University), Roberto Yus (University of California Irvine), Anupam Dasy (Carnegie Mellon University), Srutik Bhagavatula (Carnegie Mellon University), William Melichery (Carnegie Mellon University), Pardis Emami Naeini (Carnegie Mellon University), Shikun Zhang (Carnegie Mellon University), Lujo Bauerei (Carnegie Mellon University), Alfred Kobza (University of California Irvine), Sharad Mehrotra (University of California Irvine), Norman Sadeh (Carnegie Mellon University), Nalini Venkatasubramanian (University of California Irvine)

The Internet of Things (IoT) is changing the way we interact with our surrounding environment in domains as diverse as health, transportation, office buildings or our homes. In smart building environments, information captured about a building’s infrastructure and its inhabitants will help develop services that can help us become more productive, increase our comfort, enhance our social interactions, increase safety, save energy and more. But by relying on the collection and sharing of information about a building’s inhabitants and their activities, these services also open the door to privacy risks. In this paper, we introduce a framework where IoT Assistants capture and manage the privacy preferences of their users and communicate them to privacy-aware smart buildings, which enforce them when collecting user data or sharing it with building services. We outline elements of an infrastructure necessary to support such interactions and also discuss important privacy policy attributes that need to be captured. This includes looking at attributes necessary to describe – (1) the data collection and sharing practices associated with deployed sensors and services in smart buildings as well as (2) the privacy preferences we need to capture to help users manage their privacy in such environments.

Deploying Data-Driven Security Solutions on Resource-Constrained Wearable IoT System
Hang Cai (Worcester Polytechnic Institute), Tianlong Yun (Worcester Polytechnic Institute), Josiah Hester (Dartmouth College), Krishna K. Venkatasubramanian (Clemson University)

Wearable Internet-of-Things (WIoT) environments have demonstrated great potential in a broad range of applications in healthcare and well-being. Security is essential for WoT environments. Lack of security in WoTs not only harms user privacy, but may also harm the user’s safety. Though devices in the WoT can be attacked in many ways, in this paper we focus on adversaries who mount what we call sensorjacking attacks, which prevent the constituent medical devices from accurately collecting and reporting the user’s health state (e.g., reporting old or wrong physiological measurements). In this paper we outline some of our experiences in implementing a data-driven security solution for detecting sensorjacking attack on a secure wearable internet-of-things (WoT) base station called the Amulet. Given the limited capabilities (computation, memory, battery power) of the Amulet platform, implementing such a security solution is quite challenging and presents several tradeoffs with respect to resources requirements. We conclude the paper with a list of insights into what capabilities constrained WoT platforms should provide developers so as to make the inclusion of data-driven security primitives on such systems easy.

A Motif based IoT Framework for Data Efficiency
Akash Sahoo (Texas A&M University), Rabi Mahapatra (Texas A&M University)

Internet of Things (IoT) has allowed embedded devices to connect to the vast Internet network worldwide. With billions of IoT devices waiting to be connected, it is necessary to build efficient infrastructure to handle large amount of data for efficient storage and network traffic. The amount of data created at the IoT edges is regarded as one the biggest challenges of IoT. This paper proposes a motif-based encoding scheme for IoT framework that helps to reduce data generated by sensors at edge nodes. This simple encoding feature resides in both the server and the end devices like in server-client model. Our experiments demonstrated the schemes benefits by using slow and fast baud rate sensors such as temperature and accelerometer respectively as the case studies. The results obtained show the proposed motif based framework reduces the data redundancy up to two orders of magnitude while retaining more than 80% accuracy towards motif recognition.

CoTWare: A Cloud of Things Middleware
Jameela Al-Jaroodi (Robert Morris University), Nader Mohamed (Middleware Technologies Lab.), Imad Jawhar (Midcomp Research Center)

There are many applications that require integrating a large number of physical objects and devices in a large-scale Internet of Things (IoT) networks. Some examples of these applications are smart grids, smart water networks, and intelligent transportation systems. These applications need real-time controls, powerful and scalable data storage and processing capabilities, and advanced data analytics mechanisms. One of the promising technologies to support such applications is the Cloud of Things (CoT). CoT can provide a platform for linking an IoT with Cloud Computing (CC). Another technology that can be utilized for enhancing IoT applications is Fog Computing, which extends the traditional Cloud Computing paradigm to the edge of the network to enable better support for operating enhanced services. However, proper integration and efficient utilization of CoT and Fog Computing for large-scale IoT applications is not an easy task. This paper proposes a service-oriented middleware, called CoTWare, to facilitate effective integration and utilization of CoT and Fog Computing for large-scale IoT applications.

Securing the Internet of Things: A Meta-Study of Challenges, Approaches, and Open Problems
Mahmoud Hossain (University of Alabama at Birmingham), Ragib Hasan (University of Alabama at Birmingham), Anthony Skjellum (Auburn University)

The Internet of Things (IoT) is becoming a key infrastructure for the development of smart ecosystems. However, the increased deployment of IoT devices with poor security has already rendered them increasingly vulnerable to cyber attacks. In some cases, they can be used as a tool for committing serious crimes. Although some researchers have already explored such issues in the IoT domain and provided solutions for them, there remains the need for a thorough analysis of the challenges, solutions, and open problems in this domain. In this paper, we consider this research gap and provide a systematic analysis of security issues of IoT-based systems. Then, we discuss certain existing research projects to resolve the security issues. Finally, we highlight a set of open problems and provide a detailed description for each. We posit that our systematic approach for understanding the nature and challenges in IoT security will motivate researchers to addressing and solving these problems. Index Terms—Internet of Things; Security Issue; Attack Sur- face; Attack Taxonomy; IoT Forensics.

Internet of Things Framework for Smart Learning Analytics
Ali Yavari (Swinburne University of Technology), Reza Soltanpoor (RMIT University)
Learning Analytics (LA) has become a prominent paradigm in the context of education lately which adopts the recent advancements of technology such as cloud computing, big data processing, and Internet of Things. LA also requires an intensive amount of processing resource to generate relevant analytical results. However, the traditional approaches have been inefficient to tackle LA challenges such as real-time, high performance, and scalable processing of heterogeneous datasets and streaming data. An Internet of Things (IoT) scalable, distributed and high performance framework has the potential to address mentioned LA challenges by efficient contextualization of data. In this paper, Smart Learning Analytics conceptual model is proposed to improve the effectiveness of LA by utilizing an IoT-based platform in terms of performance, scalability, and efficiency.
Heterogeneous Malware Spread Process in Star Network
Libo Jiao (Tsinghua University), Hao Yin (Tsinghua University), Dongchao Guo (Tsinghua University), Yongqiang Lyu (Tsinghua University)

The heterogeneous SIS model for virus spread in any finite size graph characterizes the influence of factors of SIS model and could be analyzed by the extended N-Intertwined model introduced in [1]. We specifically focus on the heterogeneous virus spread in the star network in this paper. The epidemic threshold and the average meta-stable state fraction of infected nodes are derived for virus spread in the star network. Our results illustrate the effect of the factors of SIS model on the steady state infection.

Cost Reduction in Hybrid Clouds for Enterprise Computing
Biyu Zhou (Institute of Computing Technology, Chinese Academy of Sciences), Fa Zhang (Institute of Computing Technology, Chinese Academy of Sciences), Jie Wu (Temple University), Zhiyong Liu (Institute of Computing Technology, Chinese Academy of Sciences)

Hybrid cloud-based deployment is a trend in cloud computing which enables enterprises to benefit from cloud infrastructures while honoring privacy restrictions on some services. Enterprise application migration is an effective way to improve the efficiency of using the cloud infrastructures. However, it is a challenging problem to decide which parts of the applications to migrate and where to migrate. In this paper, we focus on the problem of planning the migration of enterprise applications in hybrid cloud infrastructures. Unlike previous studies, we consider a general hybrid cloud architecture that involves multiple public clouds rather than only one. Our aim is to maximize the enterprise cost reduction under the constraint of user experience in terms of response time. We first formulate the application migration problem as an optimization problem. Aware of its NP-hardness, we design an efficient migration framework to approximate the optimum for a large problem size. First, we leverage the application characteristic to reduce the scale of the problem by dividing it into multiple smaller subproblems. Then, an efficient algorithm based on dynamic programming is proposed to solve the small scale subproblems. Finally, we construct a feasible solution to the original problem. Simulation results demonstrate that our framework can bring significant benefits to enterprises.

DC-RSF: A Dynamic and Customized Reputation System Framework for Joint Cloud Computing
Fanghua Ye (Sun Yat-sen University), Zibin Zheng (Sun Yat-sen University), Chuan Chen (Sun Yat-sen University), Yuren Zhou (Sun Yat-sen University)

Joint cloud computing (JointCloud), as a brand-new paradigm of cloud computing, aims at building a cloud ecosystem, in which end users are agnostic to cloud service vendors as applications and services are built upon virtual clouds. In case of low quality cloud resources provided deliberately and in order to facilitate the persistent and sound development of JointCloud ecosystem, we propose a dynamic and customized reputation system framework (DC-RSF) to evaluate the credibility of cloud service vendors. At the core of DC-RSF is the customized and dynamic credibility model (CDCM), which calculates credit value for each cloud service vendor based on service requirements of end users and credential attributes of cloud service vendors. We further incorporate a Blockchain-based module into DC-RSF to prevent the credit value from being artificially tampered.

Web Service Appliance Based on Unikernel
Kai Yu (National Lab for Parallel and Distributed Processing), Chengfei Zhang (National Lab for Parallel and Distributed Processing), Yunxiang Zhao (National Lab for Parallel and Distributed Processing)

Mini-OS is a tiny OS (operating system) kernel distributed with Xen Project Hypervisor. It is mainly used as an OS for stub domain aimed at Dom0 disaggregation and also a stepping stone for Unikernel development. We implemented a simple http server on Mini-OS, and built Mini-OS into a web service appliance. We evaluated its performance compared with the same implemented server on Ubuntu PV (para-virtualization) DomU, and achieved about 39% performance improvement. The results show that Mini-OS can be a web service appliance and has a good performance.

Analysis and Evaluation of the GAS Model for Distributed Graph Computation
Wang Jinyan (National Lab for Parallel and Distributed Processing), Zhang Chengfei (National Lab for Parallel and Distributed Processing)

Compared with distributed graph computation, traditionally single node computation is unfitted in processing large scale graph data. The GAS (Gather, Apply and Scatter) Model is a universal vertex-cut graph computation programming model based on edge-centric programs to support graph algorithms, which process distributed graph computation after graph partition. In this paper, we introduce that three minor-steps of GAS. We then analyze more complete process of GAS considering intra-node computation and inter-node communication of distributed graph computation. Based on our analysis, we evaluate the performance in different nodes of graph analysis algorithm applying GAS model. The evaluation shows that the bottleneck is computation performance or communication bandwidth depending on number of nodes, which is an inspiration of optimizing the GAS model.

Traffic Signs Detection Based on Faster R-CNN
Zhongrong Zuo (National Lab for Parallel and Distributed Processing), Kai Yu (National Lab for Parallel and Distributed Processing), Qiao Zhou (National Lab for Parallel and Distributed Processing), Xu Wang (National Lab for Parallel and Distributed Processing), Ting Li (National Lab for Parallel and Distributed Processing)

In this paper, we use a advanced method called Faster R-CNN to detect traffic signs. This new method represents the highest level in object recognition, which don't need to extract image feature manually anymore and can segment image to get candidate region proposals automatically. Our experiment is based on a traffic sign detection competition in 2016 by CCF and USEE company. The mAP value of the result is 0.3449 that means Faster R-CNN can indeed be applied in this field. Even though the experiment did not achieve the best results, we explore a new method in the area of the traffic signs detection. We believe that we can get a better achievement in the future.

JCLedger: A Blockchain Based Distributed Ledger for JointCloud Computing
With the development of Economic Globalization, traditional single-cloud providers can not meet the needs of the explosive, global, diverse cloud services. JointCloud aims at empowering the cooperation among multiple Cloud Service Providers (CSP) to provide cross-cloud services. Our work in this paper is mainly focused on the accounting technology for JointCloud computing and we propose the JCLedger - a blockchain based distributed ledger. A new participant CCP (Cryptocurrency Provider) is introduced into the JointCloud collaboration environment to provide the cryptocurrency transferred. We have a detailed description of JCLedger model. We further analyze the four most important mechanisms for JCLedger and provide basic perspectives for in-depth analysis. Finally, we discuss the innovations of JCLedger and our future work in this field.

Corporation Architecture for Multiple Cloud Service Providers in JointCloud Computing

Peichang Shi (National University of Defense Technology), Huaimin Wang (National University of Defense Technology), Xikun Yue (National University of Defense Technology), Shilian Yang (National University of Defense Technology), Shangzhi Yang (National University of Defense Technology), Yuxing Peng (National University of Defense Technology)

Nowadays, cloud computing is hard to effectively sustain the implementation of the commercial model of Internet Service globalization. There is a growing trend to build an environment of cloud service, with the capacity to serve anytime and anywhere, by mutual cooperation between cloud service providers around the world. However, this tendency will raise a key issue which is how to provide a benign environment, that allows self-collaboration and fair competition, for different cloud service providers with diverse stakeholder. Guided by the concept and structure of Service-Oriented Architecture (SOA) service, this paper proposes a structure named JointCloud Corporation Environment (JCCE), which offers a mutual benefit and win-win JointCloud environment for global cloud service providers. JCCE contains three core services, which are Distributed Cloud Transaction, Distributed Cloud Community and Distributed Cloud Supervision. Also, facing with different cloud service participants, JCCE offers three main service modes for their consumption, supply and coordination. This study plays a significant role in supporting the sharing and self-collaboration of multiple cloud entities, and promoting the development of cloud service market healthy and orderly.

Sharing Privacy Data in Semi-Trustworthy Storage through Hierarchical Access Control

Yuzhao Wu (Tsinghua University), Yongqiang Lyu (Tsinghua University), Qian Fang (Tsinghua University), Geng Zheng (Tsinghua University), Hao Yin (Tsinghua University), Yuanchun Shi (Tsinghua University)

Data outsourcing in cloud is emerging as a successful paradigm that benefits organizations and enterprises with high-performance, low-cost, scalable data storage and sharing services. However, this paradigm also brings forth new challenges for data confidentiality because the outsourced are not under the physic control of the data owners. The existing schemes to achieve the security and usability goal usually apply encryption to the data before outsourcing them to the storage service providers (SSP), and disclose the decryption keys only to authorized user. They cannot ensure the security of data while operating data in cloud where the third-party service providers are usually semi-trustworthy, and need lots of time to deal with the data. We construct a privacy data management system appending hierarchical access control called HAC-DMS, which can only ensure not only security but also save plenty of time when updating data in cloud.

A Reliability Benchmark for Big Data Systems on JointCloud

Yingying Zheng (Institute of Software, Chinese Academy of Sciences), Lijie Xu (Institute of Software, Chinese Academy of Sciences), Wei Wang (Institute of Software, Chinese Academy of Sciences), Wei Zhou (KSYUN), Ying Ding (Changchun University of Science and Technology)

JointCloud provides a flexible and elastic computing resource platform. Big data systems such as MapReduce and Spark are widely deployed on this platform for big data processing. These frameworks have high scalability, but the applications running atop them often generate runtime errors, such as out of memory errors, IOExceptions, and task timeouts. For users, they want to know whether the developed applications have potential application faults. For system designers and managers, they want to know whether the deployed/updated frameworks have potential system faults. Current performance benchmarking can choose suitable clouds platform for customers. However, they do not consider reliability of applications deployed on the cloud. In addition, current benchmarks for big data system are also only designed for performance testing. To fill this gap, we propose a reliability benchmark, which contains representative applications, an abnormal data generator, and a configuration combination generator. Different from performance benchmarks, this benchmark (1) generates abnormal test data according to the application characteristics, and (2) reduces the configuration combination space based on configuration features. Currently, we implemented this benchmark on Spark framework. In our preliminary test, we found three types of errors (i.e., out of memory error, timeout and wrong results) in five SQL, Machine Learning, and Graph applications.

UCPR:User Classification and Influence Analysis in Social Network

Cong Zha (Tsinghua University), Yongqiang Lv (Tsinghua University)

There are vigorous developments of social network which affect out life greatly. User influence is an important reason to pro-mote the interaction in social network. When we analyze user influence, single value can’t indicate the user influence in different domains. This paper puts forward the design of User Classification PageRank (UCPR) to solve this problem. Firstly, we classify users according to the content which they forwarded. Then, we use space mapping to set up several subnet. Finally, we analyze user influence in every specific subnet by Domain Mapped Network (DMN) which is based on PageRank algorithm and we improve this algorithm to analyze the user influence in different domains. Through the work of this paper, we used a vector to present user influence rather than a single number and we test and verified the long-tailed distributions of social net-work in experiments.

Adaptive Routing Algorithm for Joint Cloud Video Delivery

Zexun Jiang (Tsinghua University), Hao Yin (Tsinghua University)

As the Internet keeps growing, online video has become a great part of the current Internet data traffic, which will take over 80% of Internet traffic according to Ciscos report. Also, new and more heavyweight applications keep developing to fulfill people’s growing requirements, like 4k resolution and visual reality videos. However, one single service provider, like a Content Delivery Network (CDN), can not meet the performance requirements completely. To employ the potential of Joint Cloud, this paper designs and implements a new request routing algorithm that can make video delivery utilize multiple clouds and servers. On the premise of guaranteeing the quality of video playing, this algorithm minimizes the cost of service resources based on different infrastructures service quality, cost, and cover
Towards Efficient Resource Management in Virtual Clouds
Bo An (Peking University), Junming Ma (Peking University), Donggang Cao (Peking University), Gang Huang (Peking University)

The use of multiple clouds brings many advantages: cost optimization, Quality-of-Service (QoS) improvements, high availability, avoidance of vendor lock-in, disaster recovery and so on. However, currently the cloud vendor is largely proprietary and different cloud vendors have their own heterogeneous infrastructure, making it difficult for users to utilize resource from multiple cloud vendors. As a result, users have to manage distributed applications spanning multiple clouds and take into consideration the services migration for reasons like best cost efficiency. In this paper, we introduce the notion of Virtual Cloud and focus on the issues related to multi-cloud resource management in Virtual Cloud. Virtual Cloud is a customized cloud by aggregating resources and services of different clouds and aims to provide end users with a specific cloud working environment. It will ease users’ burden of resource and distributed application management as well as the workload migration across cloud.

Monitoring and Billing of A Lightweight Cloud System Based on Linux Container
Yujian Zhu (Peking University), Junming Ma (Peking University), Bo An (Peking University), Donggang Cao (Peking University)

Nowadays, more and more enterprises and research institutes choose to build mini-datacenters and deploy private cloud environments to meet growing business and research needs. To make users can run different application frameworks on the same datacenter, Cao et al. proposed a new service model named ClaS (Cluster as a Service) and developed a lightweight prototype system named Docklet which is based on LXC (Linux Container). Docklet faces a problem of resources waste and abuse due to our free policy. This paper introduces the monitoring and billing modules of Docklet in order to solve this problem. Monitoring module provides users and administrators with a clear, real-time and detailed monitoring interface to understand the statues of running applications and the usage of physical resources. Billing module uses these data to remind users to release unnecessary resources. An experiment and observations show that our proposed monitoring method is effective and lightweight and our proposed billing model increases the utilization of physical resources of a mini-datacenter.

Building emulation framework for non-volatile memory
Guoliang Zhu (National University of Defense Technology), Kai Lu (National University of Defense Technology), Xiaoping Wang (National University of Defense Technology)

Currently, researchers use simulators to experiment their innovation on emerging non-volatile memory. Unfortunately, simulation method is both time-consuming and are hard to debug. In this paper, we present a non-volatile memory emulator which enables system-level research on emerging memory. Our emulator uses performance monitoring units on off-the-shelf processors to implement an accurate performance model.

SelfFlow: Efficient Flow Scheduling for Data-Parallel Jobs
Qiao Zhou (National Lab for Parallel and Distributed Processing), Ziyang Li (National Lab for Parallel and Distributed Processing), Ping Zhong (Central South University), Tian Tian (National Lab for Parallel and Distributed Processing), Yuxing Peng (National Lab for Parallel and Distributed Processing)

Data-parallel jobs transfer massive amounts of data between a series of successive stages. The coflow abstraction is proposed to represent a group of parallel flows between two stages and efficiently improves stagelevel performance. However, state-of-the-art coflow scheduling techniques are agnostic to the jobs' intercoflow semantics and thus are suboptimal in reducing the average job completion times (JCT). To address this problem, in this paper we present the “semantic flow” (selfow) abstraction to express the job-level intercoflow semantics. A selfow comprises not only all the coflows of a job but also the relationship between the coflows. We design an efficient selfow scheduler which utilizes the rich selfow semantics of jobs to achieve better performance than selfow-agnostic scheduling for data parallel jobs.

Online Encoding for Erasure-Coded Distributed Storage Systems
Fangliang Xu (National University of Defense Technology), Yijie Wang (National University of Defense Technology), Xingkong Ma (National University of Defense Technology)

Many large-scale distributed storage systems deploy erasure coding to protect data from frequent server failures for cost reason. In most of these systems, newly inserted data is first replicated across different storage nodes and then migrated to erasure coded. Although this offline encoding manner can improve performance of data access before erasure coding for some systems, it helps little and wastes many network resources and disk resources for many other systems. In this study, we propose an online encoding method, which encodes data as soon as it is inserted into the system. By eliminating the migration process, our online encoding can significantly reduce network transfer and data read; by caching the intermediate parity blocks into memory, our online encoding also significantly reduce data write. Analysis show that our online encoding can reduce data transfer by more than 25%, reduce data write by 57% at least and eliminate all data read, compared to traditional offline encoding.
PED 2017 Workshop Abstracts

Bruno Padilha (University of Sao Paulo), André Luis Schwerz (Federal University of Technology), Rafael Liberato Roberto (Federal University of Technology)

Despite the significant evolution of the design and implementation of business process models, a transactional approach that evolves an incremental and adaptive strategy remains an important challenge to be overcome. Traditional frameworks such as BPEL, Process Algebra, and Petri Net require an additional software layer or some third party toolkits to be able to enforce a data-state based transaction control and deal with semantic exceptions. However, the complexity of implementation based on these traditional frameworks, especially to treat exceptions, is too high. In this paper, we present the WED-SQL, a distributed framework that provides a reliable and efficient way to design and implement business processes. Our main contribution is the integration of WED-flow concepts into the PostgreSQL RDBMS. This integration enables the WED-SQL to take full advantage of transactional properties and also benefit from the SQL language to specify the WED-flow definitions.

**Querying Workflow Logs**
Yan Tang (University of California at Santa Barbara), Jianwen Su (University of California at Santa Barbara)

A business process (BP or workflow) is an assembly of tasks to accomplish a business goal. Business process management (BPM) is a study to provide support for the design, configuration/implementation, enactment and monitoring, diagnose/analysis, and re-design of workflow. Business analytics or intelligence (BI) is a necessary step towards re-design/improvement. The traditional methodology for BI is the well known sequence of ETL, data/process warehouse, and OLAP tools. In this paper, we focus on the problem of ad hoc querying process enactments for data-centric business processes. We develop an algebraic query language based on “incidents” to allow the user to formulate ad hoc queries directly on workflow logs. A formal semantics and an preliminary query evaluation algorithm are provided.

**On the integration of event-based and transaction-based architectures for Supply Chains**
Zhijie Li (Indiana University–Purdue University Indianapolis), Haoyan Wu (Indiana University–Purdue University Indianapolis), Brian King (Indiana University–Purdue University Indianapolis), Zina Ben-Miled (Indiana University–Purdue University Indianapolis), John Wassick (The Dow Chemical Company), Jeffrey Tazelaar (The Dow Chemical Company)

Affordable and reliable supply chain visibility is becoming increasingly important as the complexity of the network underlying supply chains is becoming orders of magnitudes higher compared to a decade ago. Moreover this increase in complexity is starting to reflect on the cost of goods and their availability to the consumers. This paper addresses two key issues in the distribution phase of the supply chain, namely, affordability and pseudo real-time visibility of truck load activities. The proposed framework creates a digital thread that tracks the pseudo real-time status of the shipment making the physical distribution process completely transparent to the stakeholders. The architecture of the framework is based on a dynamic hybrid peer-to-peer network and a private/public blockchain data model that leverages emergent sensor technologies.

**CacheDOCS: A Dynamic Key-Value Object Caching Service**
Julien Gascon-Samson (University of British Columbia), Michael Coppinger (McGill University), Fan Jin (McGill University), Jörg Kienzle (McGill University), Bettina Kemme (McGill University)

Caching plays an important role in many domains, as it can lead to important performance improvements. A key-value based caching system typically stores the results of popular queries in efficient storage location. While caching enjoys widespread usage in the context of dynamic web applications, most mainstream caching systems store static binary items, which makes them impractical for many real-world applications that would benefit from storing dynamic items. In this paper, we propose CacheDOCS, a dynamic key-value object caching service that allows for caching arbitrary objects. As part of our model, CacheDOCS provides an API that supports the execution of operations against cached objects, and allows for clients to seamlessly subscribe to keep their local copies in sync with cached remote objects. CacheDOCS supports multiple update dissemination strategies in order to optimize performance, and proposes a versioning mechanism to ensure consistency. We implemented a full version of CacheDOCS and we ran several performance-related experiments under three use-case scenarios.
A novel game-theoretic model for content-adaptive image steganography
Qi Li (Hunan University), Xin Liao (Hunan University), Guoyong Chen (Hunan University), Liping Ding (Guangzhou Branch of Institute of Software, Chinese Academy of Science)

Content-adaptive image steganography means that steganographer chooses security embedding positions based on image textures. Steganalyst can also focus on detecting these positions according to image textures. Game theory is preferred to analyze the above situation. However, in previous game models, steganalyst will mistakenly identify that no bit is embedded, when the secret bit is the same as the least significant bit of cover image. In this paper, a novel gametheoretic model based on secondary embedding is proposed to correct the judgment drawback for a better Nash equilibrium by steganalyst. However, steganalyst’s choice disturbs previous equilibrium and steganographer will change his choice to find new equilibrium by Game theory. Co-occurrence matrix and point deviation degree are utilized for describing steganalyst’s choices. The occurrence number of each pixel pairs is calculated to constitute co-occurrence matrix, and then Euclidean distance between one point and adjacent points is computed to locate embedding positions. In content-adaptive image steganography, we can draw a conclusion that steganographer should select embedding positions from both image edge areas and smooth areas.

A Fine-grained Access Control Scheme for Big Data Based on Classification Attributes
Tengfei Yang (State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences), Peisong Shen (State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences), Xue Tian (State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences), Chi Chen (State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences)

In order to protect the security and privacy of big data, the cloud storage service needs to enforce effective access control mechanism on user requests. Attribute-Based Encryption is a promising cryptographic access control technique to ensure the end-to-end security of data in cloud. However, the existing ABE researches mainly focus on the efficiency decryption, while the flexibility of policy, the communication cost, and the metadata management of ciphertexts are still challenging issues in the big data environment. In this paper, for the first time, we propose a new distributed, scalable and fine-grained access control scheme based on classification attributes for the cloud object storage. The classification attributes and threshold policies are integrated into an access structure, and then the objects are encrypted with the integrated access structure. The constant-size ciphertext components related to attributes can be managed as the corresponding metadata. As a result the encryption complexity and ciphertext storage are reduced. In addition, we present a new label-based access control model with multi-authorities to describe the detailed relationships of entities in our scheme. Besides, the proposed scheme is proved to be secure under IBDHE assumption, and the system implementation demonstrates the practical feasibility and good performance.

Social-Aware Decentralization for Efficient and Secure Multi-Party Computation
Yuzhe Tang (Syracuse University), Sucheta Soundarajan (Syracuse University)

This work studies the problem of MPC scheduling that is, identifying a set of computing nodes to execute secure multi-party computation protocols (MPC) over a distributed private dataset. Our primary contribution is in estimating the risk of collusion between nodes to whom the computation is scheduled. This work has potential in enabling efficient privacy-preserving data sharing in emerging platforms of big-data federation, in healthcare, finance, and other marketplaces. In our methods, we assume that the MPC computing nodes exist in a social network, and present two models for estimating the risk of collusion, as well as algorithms for finding the MPC nodes such that the risk of collusion is minimized. We evaluate our methods on several real-world network datasets, and show that they are effective in minimizing the risk levels.

Statistical Anomaly Detection on Metadata Streams via Commodity Software to Protect Company
Christine Chen (University of Portland), James Gurganus (Micro Systems Engineering, Inc.)

As a company grows, its infrastructure naturally must grow to support it. The resulting mountains of infrastructure metadata contain valuable information on the health and wellbeing of the systems through the company. For example, an abnormally low disk write rate to a file server may indicate that a regularly scheduled task has failed to start, or an abnormally high disk write rate may indicate the presence of a malicious threat such as ransomware. The hypothesis of this case study is that such metadata streams can be effectively utilized by implementing statistical anomaly detection methods via commodity software (Splunk, in this case). These methods were tested primarily on server metadata in a ransomware simulation and also on server metadata from file servers and production servers in active use.

In the ransomware simulation, the alerting system detected the ransomware behavior five minutes after an encryption event began in the simulation environment and alerted steadily for the duration of the simulation. In the week-long experiment over 11 file servers and production servers, a total of 1,484 alerts were generated. Applying simple correlation techniques created a more concentrated information stream with 77 events. These results confirm the value of metadata in identifying system anomalies and providing another layer of defense against malicious threats. The relatively simple anomaly detection techniques utilized in this case study also highlight the increasing practicality of behavioral analyticsthat can only be a matter of time before such techniques will be ubiquitous.

Computational improvements in parallelized k-anonymous microaggregation of large databases
Ahmad Mohamad Mezher (Universitat Politècnica de Catalunya), Alejandro García Álvarez (Universitat Politècnica de Catalunya), David Rebollo-Monedero (Universitat Politècnica de Catalunya), Jordi Forné (Universitat Politècnica de Catalunya)

The technical contents of this paper fall within the field of statistical disclosure control (SDC), which concerns the postprocessing of the demographic portion of the statistical results of surveys containing sensitive personal information, in order to effectively safeguard the anonymity of the participating respondents. The concrete purpose of this study is to improve the efficiency of a widely used algorithm for k-anonymous microaggregation, known as maximum distance to average vector (MDAV), to vastly accelerate its execution without affecting its excellent functional performance with respect to competing methods. The improvements put forth in this paper encompass algebraic modifications and the use of the basic linear algebra subprograms (BLAS) library, for the efficient parallel computation of MDAV on CPU.
WoSC 2017 Workshop Abstracts

Ripple: Home Automation for Research Data Management
Ryan Chard (Argonne National Laboratory), Kyle Chard (University of Chicago and Argonne National Lab), Jason Alt (National Center for Supercomputing Applications), Dilworth Parkinson (Lawrence Berkeley National Laboratory), Steve Tuecke (University of Chicago and Argonne National Lab), Ian Foster (Argonne National Laboratory & The University of Chicago)

Exploding data volumes and acquisition rates, plus ever more complex research processes, place significant strain on research data management processes. It is increasingly common for data to flow through pipelines comprised of dozens of different management, organization, and analysis steps distributed across multiple institutions and storage systems. To alleviate the resulting complexity, we propose a home automation approach to managing data throughout its lifecycle, in which users specify high-level rules the actions that should be performed on data at different times and locations. To this end, we have developed RIPLE, a responsive storage architecture that allows users to express data management tasks via a rules notation. RIPLE monitors storage systems for events, evaluates rules, and uses serverless computing techniques to execute actions in response to these events. We evaluate our solution by applying RIPLE to the data lifecycle of two real-world projects, in astronomy and light and source science, and show that it can automate many mundane and cumbersome data management processes.

Pipsqueak: Lean Lambdas with Large Libraries
Edward Oakes (University of Wisconsin-Madison), Leon Yang (University of Wisconsin-Madison), Kevin Houck (University of Wisconsin-Madison), Tyler Harter (Microsoft Gray Systems Lab), Andrea C. Arpaci-Dusseau (University of Wisconsin-Madison), Remzi H. Arpaci-Dusseau (University of Wisconsin-Madison)

Microservices are usually fast to deploy because each microservice is small, and thus each can be installed and started quickly. Unfortunately, lean microservices that depend on large libraries will start slowly and harm elasticity. In this paper, we explore the challenges of lean microservices that rely on large libraries in the context of Python packages and the OpenLambda serverless computing platform. We analyze the package types and compressibility of libraries distributed via the Python Package Index and propose PipBench, a new tool for evaluating package support. We also propose Pipsqueak, a package-aware compute platform based on OpenLambda.

Leveraging the Serverless Architecture for Securing Linux Containers
Nilton Bila (IBM), Paolo Dettori (IBM), Ali Kanso (IBM), Yuji Watanabe (IBM), Alaa Youssef (IBM)

Linux containers present a lightweight solution to package applications into images and instantiate them in isolated environments. Such images may include vulnerabilities that can be exploited at runtime. A vulnerability scanning service can detect these vulnerabilities by periodically scanning the containers and their images for potential threats. When a threat is detected, an event may be generated to (1) quarantine or remove the compromised container(s) and optionally (2) remedy the vulnerability by rebuilding a secure image. We believe that such event-driven process is a great fit to be implemented in a serverless architecture. In this paper we present our design and implementation of a serverless security analytics service based on OpenWhisk and Kubernetes.

Serverless Computing: Design, Implementation, and Performance
Garrett McGrath (University of Notre Dame), Paul R. Brenner (University of Notre Dame)

We present the design of a novel performance-oriented serverless computing platform implemented in .NET, deployed in Microsoft Azure, and utilizing Windows containers as function execution environments. Implementation challenges such as function scaling and container discovery, lifecycle, and reuse are discussed in detail. We propose metrics to evaluate the execution performance of serverless platforms and conduct tests on our prototype as well as AWS Lambda, Azure Functions and IBM’s deployment of Apache OpenWhisk. Our measurements show the prototype achieving greater throughput than other platforms at most concurrency levels, and we examine the scaling and instance expiration trends in the implementations. Additionally, we discuss the gaps and limitations in our current design, propose possible solutions, and highlight future research.
Accelerating Big Data Infrastructure and Applications
Kevin Brown (Tokyo Institute of Technology), Tianqi Xu (Tokyo Institute of Technology), Keita Iwabuchi (Tokyo Institute of Technology), Kento Sato (Lawrence Livermore National Laboratory), Adam Moody (Lawrence Livermore National Laboratory), Kathryn Mohror (Lawrence Livermore National Laboratory), Nikhil Jain (Lawrence Livermore National Laboratory), Abhinav Bhatte (Lawrence Livermore National Laboratory), Martin Schulz (Lawrence Livermore National Laboratory), Roger Pearce (Lawrence Livermore National Laboratory), Maya Gokhale (Lawrence Livermore National Laboratory), Satoshi Matsuoka (Tokyo Institute of Technology)

High-performance computing (HPC) systems are increasingly being used for data-intensive, or “Big Data”, workloads. However, since traditional HPC workloads are compute-intensive, the HPC-Big Data convergence has created many challenges with optimizing data movement and processing on modern supercomputers. Our collaborative work addresses these challenges using a three-pronged approach: (i) measuring and modeling extreme-scale I/O workloads, (ii) designing a low-latency, scalable, on-demand burst-buffer solution, and (iii) optimizing graph algorithms for processing Big Data workloads. We describe the three areas of our collaboration and report on their respective developments.

Disaster Network Evolution Using Dynamic Clustering of Twitter Data
Krishna Kant (Temple University), Yilang Wu (Aizu University), Shanshan Zhang (Temple University), Junbo Wang (Aizu University), Amitangshu Pal (Temple University)

Ad hoc smartphone networks can be used to augment communications degraded by disasters provided that the individual ad hoc clusters can reach some “connection gateways” to get out to the Internet via connected devices in the surrounding area (in addition to connectivity via any specially deployed emergency equipment). The disconnected areas are not known until they are back online; however, we need a mechanism to determine them so that the gateway device can be best recruited to provide the connectivity. This needs to be done in a dynamic environment because of disaster related mobility. In this paper we propose a mechanism to solve this problem by estimating regions that are likely to be dense but disconnected with significant number of connected devices around them. Because of lack of direct information on people (or smartphone) density, we attempt to do this by analyzing the twitter data. By virtue of its efficiency, the algorithm can be used on a dynamically evolving data set and thus allows dynamic tracking.

Single-epoch supernova classification with deep convolutional neural networks
Akisato Kimura (NTT), Ichiro Takahashi (Kavli IPMU, The University of Tokyo), Masaomi Tanaka (National Astronomical Observatory of Japan), Naoki Yasuda (Kavli IPMU, The University of Tokyo), Naonori Ueda (NTT), Naoki Yoshida (Kavli IPMU, The University of Tokyo)

Supernovae Type-Ia (SNeIa) play a significant role in exploring the history of the expansion of the Universe, since they are the best-known standard candles with which we can accurately measure the distance to the objects. Finding large samples of SNeIa and investigating their detailed characteristics has become an important issue in cosmology and astronomy. The current photometric supernova surveys produce vastly more candidates than can be followed up spectroscopically, highlighting the need for effective classification methods. Existing methods relied on a photometric approach that first measures the luminance of supernova candidates precisely and then fits the results to a parametric function of temporal changes in luminance. However, it inevitably requires a lot of observations and complex luminance measurements. In this work, we present a novel method for detecting SNeIa simply from single-shot observation images without any complex measurements, by effectively integrating the state-of-the-art computer vision methodology into the standard photometric approach. Our method first builds a convolutional neural network for estimating the luminance of supernovae from telescope images, and then constructs another neural network for the classification, where the estimated luminances and observation dates are used as features for classification. Both of the neural networks are integrated into a single deep neural network to classify SNeIa directly from observation images. Experimental results show the effectiveness of the proposed method and reveal classification performance comparable to existing photometric methods with many observations.

Enabling Large Scale Deliberation using Ideation and Negotiation-Support Agents
Katsuhide Fujita (Tokyo University of Agriculture and Technology), Takayuki Ito (Nagoya Institute of Technology), Mark Klein (MIT)

This paper describes an ongoing Japan-US project that is developing the kind of advanced computer support for online crowd-scale deliberation that is needed to enable smarter and more connected communities. Our shared work has focused on addressing both these problems: (1) ideation: helping crowds more effectively develop potential win-win solutions, and (2) decision-making: helping crowds get to pareto-optimality in the solutions they select. In Japan, a discussion support system called COLLAGREE that facilitates free text discussions to achieve consensus has been developing. In US, an online tool called the Deliberatorium that integrates argumentation theory and social computing techniques to enable more effective crowd-scale deliberation has been developing. One of our immediate joint work is to integrate the facilitated free-text discussions of COLLAGREE with the structured deliberations provided by the Deliberatorium. We will also develop automated agents that enable better ideation as well as better decision-making.
Local Information

Maps
Restaurants in/near Lenox Mall

Sprinkles Cupcakes and Ice Cream
#493 of 2,662 Restaurants in Atlanta
80 reviews
3393 Peachtree Rd NE
0.0 miles from Lenox Square
“Very Average” 04/02/2017
“The hype of a average cupcake” 03/31/2017
Cuisines: American

True Food Kitchen
#104 of 2,662 Restaurants in Atlanta
275 reviews
3393 Peachtree Rd NE Lenox Square Mall
0.0 miles from Lenox Square
“Excellent food!” 05/01/2017
“Deliciously Fresh” 04/30/2017
Cuisines: American

The Cheesecake Factory
#85 of 2,662 Restaurants in Atlanta
575 reviews
3393 Peachtree Rd NE Suite 3076A, Lenox Square Mall
0.0 miles from Lenox Square
“Hostess” 04/15/2017
“Food ok, cheesecake paradise!” 04/07/2017
Cuisines: Italian, American

Zinburger Wine & Burger Bar
#107 of 2,662 Restaurants in Atlanta
201 reviews
3393 Peachtree Rd NE Lenox Mall
0.0 miles from Lenox Square
“Very good burger” 04/27/2017
“Very good, but pricey burgers!” 04/24/2017
Cuisines: American, Bar, Wine Bar
### Dantanna’s

**#210 of 2,662 Restaurants in Atlanta**

![Grilled meat and vegetables](image)

- **5 out of 5 stars**
- **266 reviews**
- **3400 Around Lenox Rd NE**
- **0.1 miles from Lenox Square**

- **“Great burgers!” 05/03/2017**
- **“Love this place” 05/02/2017**

Cuisines: American, Bar

### Lenox Square

**#627 of 2,662 Restaurants in Atlanta**

![Interior view of a shopping mall](image)

- **4 out of 5 stars**
- **24 reviews**
- **3393 Peachtree Rd NE**
- **0.1 miles from Lenox Square**

- **“...mall” 01/17/2017**
- **“Business” 10/25/2016**

Cuisines: Fast Food

### Garrett Popcorn Shops

**#826 of 2,662 Restaurants in Atlanta**

![Popcorn bag](image)

- **4 out of 5 stars**
- **17 reviews**
- **3393 Peachtree Rd NE Lenox Square Mall**
- **0.1 miles from Lenox Square**

- **“Love the pecan popcorn” 04/12/2017**
- **“It's ok. Not like Chicago's!” 01/05/2017**

### Haagen-Dazs Shop

**#1,261 of 2,662 Restaurants in Atlanta**

- **4 out of 5 stars**
- **1 review**
- **3393 Peachtree Rd NE**
- **0.1 miles from Lenox Square**

- **“O melhor sorvete do mundo” 05/24/2014**
Bantam + Biddy
#1,334 of 2,662 Restaurants in Atlanta
19 reviews
3393 Peachtree Rd NE Unite 3065B
0.1 miles from Lenox Square
"Well prepared food, and though..." 02/21/2017
"Banana pecan waffles...yum!" 02/19/2017

Corner Bakery Cafe
#1,450 of 2,662 Restaurants in Atlanta
22 reviews
3393 Peachtree Rd NE #4033
0.1 miles from Lenox Square
"Excellent breakfast" 02/25/2017
"Dessert" 02/19/2017
Cuisines: American, Cafe, Healthy, Soups

Taziki's
#1,520 of 2,662 Restaurants in Atlanta
6 reviews
3393 Peachtree Rd NE # 10008
0.1 miles from Lenox Square
"Good choice of salads" 01/22/2017
"Consistently quite good meals..." 01/19/2017

Seven Lamps
#151 of 2,662 Restaurants in Atlanta
176 reviews
3400 Around Lenox Rd NE
0.1 miles from Lenox Square
"Say "No" to the oysters" 05/01/2017
"Great place!" 04/26/2017
Cuisines: American
Farmer's Basket

#1.263 of 2,662 Restaurants in Atlanta
Rating: 4.5/5 (12 reviews)
3393 Peachtree Rd NE Ste 1012
0.1 miles from Lenox Square

“Really good food court option...” 04/29/2017
“Great quality and quantity!” 04/06/2017
Cuisines: Fast Food

Zinburger Wine and Burger Bar

#2 of 5 Restaurants in Buckhead
Rating: 4.5/5 (7 reviews)
3393 Peachtree Road NE, Room 3065A outside entrance - Lenox Mall
0.1 miles from Lenox Square

“Great burgers, wine and salads...” 04/13/2017
“Disappointed” 03/05/2017

Panera Bread

#876 of 2,662 Restaurants in Atlanta
Rating: 4.5/5 (22 reviews)
3393 Peachtree Rd NE
0.1 miles from Lenox Square

“dined with jade and chantel 3...” 03/26/2017
“Good Visit’ 02/12/2017
Cuisines: Soups, Cafe

Cinnabon

#989 of 2,662 Restaurants in Atlanta
Rating: 4.5/5 (5 reviews)
3393 Peachtree Rd NE Ste 1004
0.1 miles from Lenox Square

“Great cinnamon rolls! Not to b...” 02/26/2017
“ME ENCANTA!” 11/17/2015