Volume 22, Issue 1
Summer/Fall '21

CECS eNEWS

Center for Embedded and Cyber-physical Systems, University of California, Irvine

Inside this Issue:

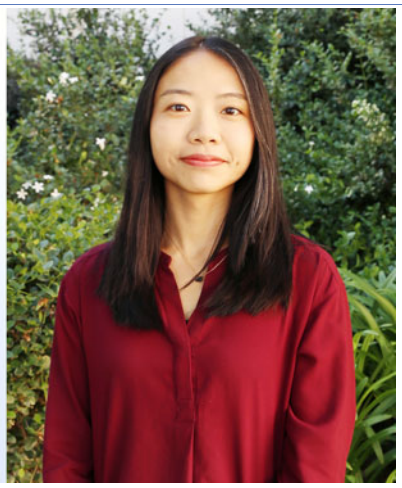
Shoukry Receives IEEE TCCPS Early-Career Award

CECS affiliated faculty, Prof. Yasser Shoukry, Assistant Professor of Electrical Engineering and Computer Science has won the IEEE Technical Committee on Cyber-Physical Systems (TCCPS) Early-Career Award for his outstanding contribution to the theory and design of safe learning-enabled cyber-physical systems. His research aims to provide novel mathematical techniques and algorithms to check that these neural networks will always make correct (or safe) decisions. The research goal is to develop algorithms and tools to reason about the resilience, security, and privacy of Artificial Intelligence (AI) controlled Cyber-Physical Systems and Internet-of-Things (IoT), in general, and robotic systems, in particular, providing a scientific basis to understand their fundamental properties and guide their design.

IEEE TCCPS recognizes a junior researcher each year from either academia or industry who has demonstrated outstanding contributions to the field of cyber-physical system (CPS) in the early stage of his/her career development.

Awards and Honors

Zhou Li and Yanning Shen won MSFT $150K Award



CECS and EECS affiliated assistant professors, Zhou Li and Yanning Shen, are working in collaboration with Microsoft to tackle the issue of spear-phishing. Li and Shen are developing a new system to automatically detect spear-phishing emails, so the damage to an individual or organization can be minimized. The researchers are planning to model the email communications as a social graph and apply graph-learning models to classify the emails. To keep the models adapted to the new benign and malicious email patterns that emerge in an organization, they will also apply online learning, a very efficient method to update the model. Their efforts are supported by a $150,000 Microsoft Security Research Artificial Intelligence Award.

Eltawil Wins Innovator of the Year Award

Professor Ahmed Eltawil's goal is to find innovative solutions that address the complexities of state-of-the-art research issues, while offering pragmatic approaches that can be easily adopted, leading to significant societal impact. Eltawil was one of the first academic groups in the world to design and build an experimental full duplex platform, and he has four patents that are cited as foundational in the field. His innovations in full duplex systems started with his initial exploratory paper in 2012, leading to the founding of his company, Lextrum in 2015, and transitioning to the acquisition of the company in early 2018. Eltawil's journey of innovation to commercialization, where research funds are used to create solid science that then creates societal value through company and job creation, is a successful example of entrepreneurship based on "Made at UCI" technology.

Rahmani and Healthcare Technology

CECS affiliated Associate Professor Amir Rahmani, as leader of HealthSciTech Group and associate director of the Institute for Future Health, is working to integrate healthcare with technology. He is currently working with a National Science Foundation grant to create a model of digital community-centered care (DCCC) with founding dean and nursing Distinguished Professor Adey Nyamathi and computer science Professor Nikil Dutt. This model would allow more monitoring in health facilities, which would allow for more health services to more people in need.

Rahmani partnered with Meals on Wheels Orange County to test the technology. Patients and caregivers are given wearable devices that monitor health measures such as heart rate or blood pressure, and they are able to communicate remotely through a mobile app.

Rahmani is currently capturing data to create individualized health models to make an effective AI for use in this health monitoring system. Rahmani and Dr. Ramesh Jain recently founded the Institute for Future Health with the aim to personalize healthcare and give the individual autonomy over their health.

As Rahmani states: “Each person is unique. The idea of personalized health is building a personal model for each patient based on what works best for them instead of prescribing the same thing to everyone.”

Student Profile

Student Profile: Arnav Malawade

Arnav Malawade received a B.S. in Computer Science and Engineering and an M.S. in Computer Engineering from the University of California Irvine (UCI) in 2018 and 2021, respectively. He is currently a Ph.D. student at UCI under the supervision of Professor Mohammad Al Faruque and is a member of the Autonomous and Intelligent Cyber-Physical Systems Lab (AICPS). His research interests include the design and security of cyber-physical systems in connected/autonomous vehicles, manufacturing, IoT, and healthcare.

In the past, he has conducted research on Industry 4.0 applications including side-channel attacks, sabotage attack detection, and predictive maintenance techniques for additive manufacturing systems such as 3D printers and DNA synthesizers. He has also researched graph-based approaches for autonomous vehicle perception, physical layer key generation for vehicle-to-everything (V2X) communication, and split-architecture computing for autonomous vehicle energy optimization. Currently he is working on developing novel methodologies for improving the energy efficiency, robustness, and safety of autonomous vehicles.

Publications

Publications

The following papers were published by CECS affiliates from July 2021 through December 2021 (and unreported papers from previous eNews).

Author, Title, Publication — Conference Proceedings

Leila Tlebaldiyeva, Galymzhan Nauryzbayev, Sultangali Arzykulov, Ahmed M. Eltawil: **Performance of NOMA-Based mmWave D2D Networks Under Practical System Conditions.** IEEE Access 9: 160958-160974, December 1-13, 2021, Virtual

Rozhin Yasaei, Shih-Yuan Yu, Emad Kasaeyan Naeini, Mohammad Abdullah Al Faruque: **GNN4IP: Graph Neural Network for Hardware Intellectual Property Piracy Detection.** DAC2021: 217-222, December 5-9, 2021, San Francisco, CA, USA

Mohanad Odema, Nafiul Rashid, Berken Utku Demirel, Mohammad Abdullah Al Faruque: **LENS: Layer Distribution Enabled Neural Architecture Search in Edge-Cloud Hierarchies.**DAC 2021: 403-408, December 5-9, 2021, San Francisco, CA, USA

Alejandro Hernández-Cano, Cheng Zhuo, Xunzhao Yin, Mohsen Imani: **RegHD: Robust and Efficient Regression in Hyper-Dimensional Learning System.** DAC2021: 7-12, December 5-9, 2021, San Francisco, CA, USA

Alejandro Hernández-Cano, Rosario Cammarota, Mohsen Imani: **PRID: Model Inversion Privacy Attacks in Hyperdimensional Learning Systems.** DAC 2021: 553-558, December 5-9, 2021, San Francisco, CA, USA

Yeseong Kim, Jiseung Kim, Mohsen Imani: **CascadeHD: Efficient Many-Class Learning Framework Using Hyperdimensional Computing.** DAC 2021: 775-780, December 5-9, 2021, San Francisco, CA, USA

Prathyush Poduval, Zhuowen Zou, Xunzhao Yin, Elaheh Sadredini, Mohsen Imani: **Cognitive Correlative Encoding for Genome Sequence Matching in Hyperdimensional System.** DAC 2021: 781-786, December 5-9, 2021, San Francisco, CA, USA

Prathyush Poduval, Zhuowen Zou, M. Hassan Najafi, Houman Homayoun, Mohsen Imani: **StocHD: Stochastic Hyperdimensional System for Efficient and Robust Learning from Raw Data.** DAC 2021: 1195-1200, December 5-9, 2021, San Francisco, CA, USA

Gaurav Kolhe, Soheil Salehi, Tyler David Sheaves, Houman Homayoun, Setareh Rafatirad, Sai Manoj P. D., Avesta Sasan: **Securing Hardware via Dynamic Obfuscation Utilizing Reconfigurable Interconnect and Logic Blocks.** DAC 2021: 229-234, December 5-9, 2021, San Francisco, CA, USA

Mingtian Tan, Zhe Zhou, Zhou Li:**The Many-faced God: Attacking Face Verification System with Embedding and Image Recovery.** ACSAC 2021: 17-30, December 6-10, 2021, Virtual

Mingxuan Liu, Yiming Zhang, Baojun Liu, Zhou Li, Haixin Duan, Donghong Sun: **Detecting and Characterizing SMS Spearphishing Attacks.** ACSAC 2021: 930-943, December 6-10, 2021, Virtual

Prathyush Poduval, Zhuowen Zou, M. Hassan Najafi, Houman Homayoun, Mohsen Imani: **StocHD: Stochastic Hyperdimensional System for Efficient and Robust Learning from Raw Data.** DAC 2021: 1195-1200, December 5-9, 2021, San Francisco, CA, USA

Febin Sunny, Asif Mirza, Mahdi Nikdast, Sudeep Pasricha: **CrossLight: A Cross-Layer Optimized Silicon Photonic Neural Network Accelerator.** DAC2021: 1069-1074, December 5-9, 2021, San Francisco, CA, USA

Publications

Publications

The following papers were published by CECS affiliates from
July 2021 through December 2021 (and unreported papers from previous eNews).

Author, Title, Publication — Conference Proceedings

Qi Han, Yu Bao, Sudeep Pasricha: **Improving Safety in Cyber Enabled Underground Mines.** NSysS 2021: 120-129, December 21-23, 2021, Cox's Bazar, Bangladesh

Adrian Dabrowski, Katharina Pfeffer, Markus Reichel, Alexandra Mai, Edgar R. Weippl, Michael Franz: **Better Keep Cash in Your Boots - Hardware Wallets are the New Single Point of Failure.**DeFi@CCS 2021: 1-8, November 19, 2021, Virtual

Chinmay Deshpande, David Gens, Michael Franz: **StackBERT: Machine Learning Assisted Static Stack Frame Size Recovery on Stripped and Optimized Binaries.** AISec@CCS 2021: 85-95, November 15, 2021, Virtual

Wenrui Lin, Berken Utku Demirel, Mohammad Abdullah Al Faruque, G. P. Li: **Energy-efficient Blood Pressure Monitoring based on Single-site Photoplethysmogram on Wearable Devices.** EMBC 2021: 504-507, November 1-5, Mexico

Berken Utku Demirel, Ivan Skelin, Haoxin Zhang, Jack J. Lin, Mohammad Abdullah Al Faruque: **Single-Channel EEG Based Arousal Level Estimation Using Multitaper Spectrum Estimation at Low-Power Wearable Devices.** EMBC 2021: 542-545, November 1-5, Mexico

Nafiul Rashid, Luke Chen, Manik Dautta, Abel Jimenez, Peter Tseng, Mohammad Abdullah Al Faruque: **Feature Augmented Hybrid CNN for Stress Recognition Using Wrist-based Photoplethysmography Sensor.** EMBC 2021: 2374-2377, November 1-5, Mexico

Omid Malekzadeh-Arasteh, Haoran Pu, Ahmad Reza Danesh, Jeffrey Lim, Po T. Wang, Charles Yu Liu, An H. Do, Zoran Nenadic, Payam Heydari: **A Fully-Integrated 1μW/Channel Dual-Mode Neural Data Acquisition System for Implantable Brain-Machine Interfaces.** EMBC 2021: 5780-5783, November 1-5, 2021, Mexico

Milad Asgari Mehrabadi, Seyed Amir Hossein Aqajari, Iman Azimi, Charles A. Downs, Nikil D. Dutt, Amir M. Rahmani: **Detection of COVID-19 Using Heart Rate and Blood Pressure: Lessons Learned from Patients with ARDS.** EMBC 2021: 2140-2143, November 1-5, 2021, Mexico

Manoj Vishwanath, Salar Jafarlou, Ikhwan Shin, Nikil D. Dutt, Amir M. Rahmani, Carolyn E. Jones, Miranda M. Lim, Hung Cao: **Investigation of Machine Learning and Deep Learning Approaches for Detection of Mild Traumatic Brain Injury from Human Sleep Electroencephalogram.** EMBC 2021: 6134-6137, November 1-5, 2021, Mexico

Ali Tazarv, Sina Labbaf, Stephanie M. Reich, Nikil D. Dutt, Amir M. Rahmani, Marco Levorato: **Personalized Stress Monitoring using Wearable Sensors in Everyday Settings.** EMBC 2021: 7332-7335, November 1-5, 2021, Mexico

Francesco Fraternali, Bharathan Balaji, Dezhi Hong, Yuvraj Agarwal, Rajesh K. Gupta: **Marble: collaborative scheduling of batteryless sensors with meta reinforcement learning.** BuildSys@SenSys 2021: 140-149, November 17-18, 2021, Coimbra, Portugal

Shuheng Li, Ranak Roy Chowdhury, Jingbo Shang, Rajesh K. Gupta, Dezhi Hong: **UniTS: Short-Time Fourier Inspired Neural Networks for Sensory Time Series Classification.** SenSys 2021: 234-247, November 15-17, 2021, Coimbra, Portugal

Publications

Publications

The following papers were published by CECS affiliates from July 2021 through December 2021 (and unreported papers from previous eNews).

Author, Title, Publication — Conference Proceedings

Omid Malekzadeh-Arasteh, Haoran Pu, Ahmad Reza Danesh, Jeffrey Lim, Po T. Wang, Charles Yu Liu, An H. Do, Zoran Nenadic, Payam Heydari: **A Fully-Integrated 1μW/Channel Dual-Mode Neural Data Acquisition System for Implantable Brain-Machine Interfaces.** EMBC 2021: 5780-5783, November 1-5, 2021, Mexico

Sina Asadi, M. Hassan Najafi, Mohsen Imani: **CORLD: In-Stream Correlation Manipulation for Low-Discrepancy Stochastic Computing.** ICCAD 2021: 1-9, November 1-4, 2021, Munich, Germany

Yeseong Kim, Mohsen Imani, Saransh Gupta, Minxuan Zhou, Tajana Simunic Rosing: **Massively Parallel Big Data Classification on a Programmable Processing In-Memory Architecture.** ICCAD 2021: 1-9, November 1-4, 2021, Munich, Germany

Jiseung Kim, Hyunsei Lee, Mohsen Imani, Yeseong Kim: **Efficient Brain-Inspired Hyperdimensional Learning with Spatiotemporal Structured Data**. MASCOTS 2021: 1-8, November 3-5, 2021, Huston, TX, USA

Prathyush Poduval, Mariam Issa, Farhad Imani, Cheng Zhuo, Xunzhao Yin, M. Hassan Najafi, Mohsen Imani**: Robust In-Memory Computing with Hyperdimensional Stochastic Representation.** NANOARCH 2021: 1-6, November 8-10, 2021, AB, Canada

Zhuowen Zou, Yeseong Kim, Farhad Imani, Haleh Alimohamadi, Rosario Cammarota, Mohsen Imani: **Scalable edge-based hyperdimensional learning system with brain-like neural adaptation.** SC 2021: 38:1-38:15, November 14-19, 2021, St. Louis, Missouri

Ali Tazarv, Marco Levorato: **A Deep Learning Approach to Predict Blood Pressure from PPG Signals.** EMBC 2021: 5658-5662, November 1-5, 2021, Mexico

Ali Tazarv, Sina Labbaf, Stephanie M. Reich, Nikil D. Dutt, Amir M. Rahmani, Marco Levorato: **Personalized Stress Monitoring using Wearable Sensors in Everyday Settings.** EMBC 2021: 7332-7335, November 1-5, 2021, Mexico

Omid Malekzadeh-Arasteh, Haoran Pu, Ahmad Reza Danesh, Jeffrey Lim, Po T. Wang, Charles Yu Liu, An H. Do, Zoran Nenadic, Payam Heydari: **A Fully-Integrated 1μW/Channel Dual-Mode Neural Data Acquisition System for Implantable Brain-Machine Interfaces.** EMBC 2021: 5780-5783, November 1-5, 2021, Mexico

Henry A. Gabb, Alexandru Nicolau, Satish Puri, Michael D. Shah, Rahul Toppur, Neftali Watkinson, Weijia Xu, Hui Zhang: **Lightning Talks of EduHPC 2021.** EduHPC@SC 2021: 43-50, November 14-14, 2021, St. Louis, MO, USA

Neftali Watkinson, Tony Givargis, Victor Joe, Alexandru Nicolau, Alexander V. Veidenbaum: **Class-Modeling of Septic Shock With Hyperdimensional Computing.** EMBC 2021: 1653-1659, November 1-5, 2021, Mexico

Neftali Watkinson, Tony Givargis, Victor Joe, Alexandru Nicolau, Alexander V. Veidenbaum: **Detecting COVID-19 Related Pneumonia On CT Scans Using Hyperdimensional Computing.** EMBC 2021: 3970-3973, November 1-5, 2021, Mexico

Tianhao Wang, Joann Qiongna Chen, Zhikun Zhang, Dong Su, Yueqiang Cheng, Zhou Li, Ninghui Li, Somesh Jha: **Continuous Release of Data Streams under both Centralized and Local Differential Privacy.** CCS 2021: 1237-1253, November 15-19, 2021, Virtual

Publications

Publications

The following papers were published by CECS affiliates from July 2021 through December 2021 (and unreported papers from previous eNews).

Author, Title, Publication — Conference Proceedings

Yiming Zhang, Baojun Liu, Chaoyi Lu, Zhou Li, Haixin Duan, Jiachen Li, Zaifeng Zhang: **Rusted Anchors: A National Client-Side View of Hidden Root CAs in the Web PKI Ecosystem.** CCS 2021: 1373-1387, November 15-19, 2021, Virtual

Fenghao Xu, Siyu Shen, Wenrui Diao, Zhou Li, Yi Chen, Rui Li, Kehuan Zhang: **Android on PC: On the Security of End-user Android Emulators.** CCS 2021: 1566-1580, November 15-19, 2021, Virtual

Jiyuan Wang, Qian Zhang, Guoqing Harry Xu, Miryung Kim: **QDiff: Differential Testing of Quantum Software Stacks.** ASE 2021: 692-704, November 15-19, 2021, Melbourne, Australia

Di Gao, Hao Lin, Zhenhua Li, Feng Qian, Qi Alfred Chen, Zhiyun Qian, Wei Liu, Liangyi Gong, Yunhao Liu: **A nation-wide census on wifi security threats: prevalence, riskiness, and the economics.**MobiCom 2021: 242-255, October 25-29, 2021, Virtual

Elaheh Sadredini, Reza Rahimi, Mohsen Imani, Kevin Skadron: **Sunder: Enabling Low-Overhead and Scalable Near-Data Pattern Matching Acceleration**. MICRO 2021: 311-323, October 18-22, 2021, Virtual

Sugil Lee, Mohammed E. Fouda, Jongeun Lee, Ahmed M. Eltawil, Fadi J. Kurdahi: **Fast and Low-Cost Mitigation of ReRAM Variability for Deep Learning Applications.** ICCD2021: 269-276, October 24-27, 2021, Storrs, CT, USA

Sultangali Arzykulov, Abdulkadir Celik, Galymzhan Nauryzbayev, Ahmed M. Eltawil: **Max-Min Fair Power Control and Coverage Probability for UAV-Assisted Cooperative and Cognitive NOMA.** ICTC 2021: 248-253, October 20-22, 2021, Jeju Island, Republic of Korea

Yerassyl Akhmetkaziyev, Galymzhan Nauryzbayev, Sultangali Arzykulov, Khaled M. Rabie, Ahmed M. Eltawil: **Ergodic Capacity of Cognitive Satellite-Terrestrial Relay Networks with Practical Limitations.** ICTC 2021: 555-560, October 20-22, 2021, Jeju Island, Republic of Korea

Sandra Hernández, José Araujo, Patric Jensfelt, Ioannis Karagiannis, Ananya Muddukrishna, Bryan Donyanavard: **Cross-layer Configuration Optimization for Localization on Resource-constrained Devices.** IROS 2021: 2282-2288, September 27-October 1, 2021

Justin Morris, Si Thu Kaung Set, Gadi Rosen, Mohsen Imani, Baris Aksanli, Tajana Rosing: **AdaptBit-HD: Adaptive Model Bitwidth for Hyperdimensional Computing.** ICCD 2021: 93-100, October 24-27, 2021, Storrs, CT, USA

Najmeh Nazari Bavarsad, Hosein Mohammadi Makrani, Hossein Sayadi, Lawrence Landis, Setareh Rafatirad, Houman Homayoun: **HosNa: A DPC++ Benchmark Suite for Heterogeneous Architectures.** ICCD 2021: 509-516, October 24-27, 2021, Storrs, CT, USA

Seongyoung Kang, Jiyoung An, Jinpyo Kim, Sang-Woo Jun: **Near-Storage Accelerator for High-Performance Log Analytics.** MICRO 2021: 434-448, October 18-22, 2021, Virtual

Sugil Lee, Mohammed E. Fouda, Jongeun Lee, Ahmed M. Eltawil, Fadi J. Kurdahi: **Fast and Low-Cost Mitigation of ReRAM Variability for Deep Learning Applications.** ICCD2021: 269-276, October 24-27, 2021, Storrs, CT, USA

Publications

Publications

The following papers were published by CECS affiliates from July 2021 through December 2021 (and unreported papers from previous eNews).

Author, Title, Publication — Conference Proceedings

Yue Yin, Emre Neftci: **Improving full-FORCE with dynamical data coupling and multilayer architecture.** BioCAS2021: 1-6, October 7-9, 2021, Berlin, Germany

Shafiur Rahman, Mahbod Afarin, Nael B. Abu-Ghazaleh, Rajiv Gupta: **JetStream: Graph Analytics on Streaming Data with Event-Driven Hardware Accelerator.** MICRO 2021: 1091-1105, October 16-20, 2021, Vitrual

Sri Shaila G, Ahmad Darki, Michalis Faloutsos, Nael B. Abu-Ghazaleh, Manu Sridharan: **DisCo: Combining Disassemblers for Improved Performance.** RAID 2021: 148-161, October 6-8, 2021, Donostia/ San Sebastian, Spain

Arthi Padmanabhan, Anand Padmanabha Iyer, Ganesh Ananthanarayanan, Yuanchao Shu, Nikolaos Karianakis, Guoqing Harry Xu, Ravi Netravali: **Towards memory-efficient inference in edge video analytics.** HotEdgeVideo@MobiCom 2021: 31-37, October 25-25, 2021, New Orleans, Louisiana

Tong Chen, Yingxiao Xiang, Yike Li, Yunzhe Tian, Endong Tong, Wenjia Niu, Jiqiang Liu, Gang Li, Qi Alfred Chen: **Protecting Reward Function of Reinforcement Learning via Minimal and Non-catastrophic Adversarial Trajectory.** SRDS 2021: 299-309, September 20-23, 2021, Chicago, IL, USA

Tianyi Zhang, Minjun Seo, Bryan Donyanavard, Nikil D. Dutt, Fadi J. Kurdahi: **Predicting Failures in Embedded Systems Using Long Short-Term Inference.** IEEE Embed. Syst. Lett. 13(3): 85-89, September 20-23, 2021

Biswadip Maity, Saehanseul Yi, Dongjoo Seo, Leming Cheng, Sung-Soo Lim, Jong-Chan Kim, Bryan Donyanavard, Nikil D. Dutt: **Chauffeur: Benchmark Suite for Design and End-to-End Analysis of Self-Driving Vehicles on Embedded Systems.** ACM Trans. Embed. Comput. Syst. 20(5s): 74:1-74:22, September 20-23, 2021

Emad Malekzadeh Arasteh, Rainer Dömer: **Improving Parallelism in System Level Models by Assessing PDES Performance.** FDL 2021: 1-7, September 8-10, 2021, Antibes, France

Ali Tazarv, Sina Labbaf, Amir M. Rahmani, Nikil D. Dutt, Marco Levorato: **Data Collection and Labeling of Real-Time IoT-Enabled Bio-Signals in Everyday Settings for Mental Health Improvement.** GoodIT 2021: 186-191, September 9-11, 2021, Roma Italy

Yerassyl Akhmetkaziyev, Galymzhan Nauryzbayev, Sultangali Arzykulov, Khaled M. Rabie, Xingwang Li, Ahmed M. Eltawil: **Underlay Hybrid Satellite-Terrestrial Relay Networks under Realistic Hardware and Channel Conditions.** VTC Fall 2021: 1-6, September 27-30, Norman, OK, USA

Minxuan Zhou, Guoyang Chen, Mohsen Imani, Saransh Gupta, Weifeng Zhang, Tajana Rosing: **PIM-DL: Boosting DNN Inference on Digital Processing In-Memory Architectures via Data Layout Optimizations.** PACT 2021: 1, September 26-29, 2021, Atlanta, GA, USA

Ali Tazarv, Sina Labbaf, Amir M. Rahmani, Nikil D. Dutt, Marco Levorato: **Data Collection and Labeling of Real-Time IoT-Enabled Bio-Signals in Everyday Settings for Mental Health Improvement.** GoodIT 2021: 186-191, September 9-11, 2021, Roma, Italy

Publications

Publications

The following papers were published by CECS affiliates from July 2021 through December 2021 (and unreported papers from previous eNews).

Author, Title, Publication — Conference Proceedings

Rebekah Houser, Shuai Hao, Zhou Li, Daiping Liu, Chase Cotton, Haining Wang: **A Comprehensive Measurement-based Investigation of DNS Hijacking.** SRDS 2021: 210-221, September 20-23, 2021, Chicago, IL, USA

Jeffrey Chen, Sehwan Hong, Warrick He, Jinyeong Moon, Sang-Woo Jun: **Eciton: Very Low-Power LSTM Neural Network Accelerator for Predictive Maintenance at the Edge.** FPL 2021: 1-8, August 30-September 3, 2021, Dresden, Germany

Shengtuo Hu, Qi Alfred Chen, Jiachen Sun, Yiheng Feng, Z. Morley Mao, Henry X. Liu: **Automated Discovery of Denial-of-Service Vulnerabilities in Connected Vehicle Protocols.** USENIX Security Symposium 2021: 3219-3236, August 11-13, 2021, Virtual

Takami Sato, Junjie Shen, Ningfei Wang, Yunhan Jia, Xue Lin, Qi Alfred Chen: **Dirty Road Can Attack: Security of Deep Learning based Automated Lane Centering under Physical-World Attack.** USENIX Security Symposium 2021: 3309-3326, August 11-13, 2021, Virtual

Jiaman Wu, Dezhi Hong, Rajesh K. Gupta, Jingbo Shang: **Sensei: Self-Supervised Sensor Name Segmentation.** ACL/IJCNLP (Findings) 2021: 1017-1027, August, 2021, Virtual

Zisong Wang, Huan Wang, Payam Heydari: **CMOS Power-Amplifier Design Perspectives for 6G Wireless Communications.** MWSCAS2021: 753-756, August 9-11, 2021, Lansing, MI, USA

Sang-Woo Jun: **Virtual avatars for instruction and student response during streaming video-based on-line teaching.** ICCSE 2021: 456-459, August 17-21, 2021, Lancaster, United Kingdom

Hadjer Benmeziane, Hamza Ouarnoughi, Kaoutar El Maghraoui, Smaïl Niar: **Accelerating Neural Architecture Search with Rank-Preserving Surrogate Models.** ArabWIC2021: 21:1-21:6, August 25-26, 2021, Sharjah, United Arab Emirates

Hadjer Benmeziane, Kaoutar El Maghraoui, Hamza Ouarnoughi, Smaïl Niar, Martin Wistuba, Naigang Wang: **Hardware-Aware Neural Architecture Search: Survey and Taxonomy.** IJCAI 2021: 4322-4329, August 11-13, 2021, Virtual

Peng Fei, Zhou Li, Zhiying Wang, Xiao Yu, Ding Li, Kangkook Jee: **SEAL: Storage-efficient Causality Analysis on Enterprise Logs with Query-friendly Compression.** USENIX Security Symposium 2021: 2987-3004, August 11-13, 2021, Virtual

Fatemah Alharbi, Arwa Alrawais, Abdulrahman Bin Rabiah, Silas Richelson, Nael B. Abu-Ghazaleh: **CSProp: Ciphertext and Signature Propagation Low-Overhead Public-Key Cryptosystem for IoT Environments.** USENIX Security Symposium 2021: 609-626, August 11-13, 2021, Virtual

Daimeng Wang, Zheng Zhang, Hang Zhang, Zhiyun Qian, Srikanth V. Krishnamurthy, Nael B. Abu-Ghazaleh: **SyzVegas: Beating Kernel Fuzzing Odds with Reinforcement Learning.** USENIX Security Symposium 2021: 2741-2758, August 11-13, 2021, Virtual

Publications

Publications

The following papers were published by CECS affiliates from July 2021 through December 2021 (and unreported papers from previous eNews).

Author, Title, Publication — Conference Proceedings

Seyed Mohammadjavad Seyed Talebi, Zhihao Yao, Ardalan Amiri Sani, Zhiyun Qian, Daniel Austin: **Undo Workarounds for Kernel Bugs.** USENIX Security Symposium 2021: 2381-2398, August 11-13, 2021, Virtual

Mohanad Odema, Nafiul Rashid, Mohammad Abdullah Al Faruque: **EExNAS: Early-Exit Neural Architecture Search Solutions for Low-Power Wearable Devices.**ISLPED 2021: 1-6, July 26-28, 2021, Boston, MA, USA

Ruochen Jiao, Hengyi Liang, Takami Sato, Junjie Shen, Qi Alfred Chen, Qi Zhu: **End-to-end Uncertainty-based Mitigation of Adversarial Attacks to Automated Lane Centering.** IV 2021: 266-273, July 11-17, 2021, Nagoya, Japan

Biswadip Maity, Bryan Donyanavard, Anmol Surhonne, Amir M. Rahmani, Andreas Herkersdorf, Nikil D. Dutt: **SEAMS: Self-Optimizing Runtime Manager for Approximate Memory Hierarchies.** ACM Trans. Embed. Comput. Syst. 20 (5): 48:1-48:26, July, 2021

Bryan Donyanavard, Tiago Mück, Kasra Moazzemi, Biswadip Maity, Caio Batista de Melo, Kenneth Stewart, Saehanseul Yi, Amir M. Rahmani, Nikil D. Dutt: **Reflecting on Self-Aware Systems-on-Chip.** A Journey of Embedded and Cyber-Physical Systems 2021: 79-95, July 1-2, 2021, Virtual

Adarsha Balaji, Shihao Song, Twisha Titirsha, Anup Das, Jeffrey L. Krichmar, Nikil D. Dutt, James A. Shackleford, Nagarajan Kandasamy, Francky Catthoor: **NeuroXplorer 1.0: An Extensible Framework for Architectural Exploration with Spiking Neural Networks.** ICONS 2021: 10:1-10:9, July 27-29, 2021, New York, NY, United States

Lingbing Yao, Hang Zhao, Jie Tang, Shaoshan Liu, Jean-Luc Gaudiot: **Streaming Data Priority Scheduling Framework for Autonomous Driving by Edge.**COMPSAC 2021: 37-42, July 12-16, 2021, Madrid, Spain

Arman Kazemi, Mohammad Mehdi Sharifi, Zhuowen Zou, Michael T. Niemier, X. Sharon Hu, Mohsen Imani: **MIMHD: Accurate and Efficient Hyperdimensional Inference Using Multi-Bit In-Memory Computing.** ISLPED 2021: 1-6, July 26-28, 2021, Boston, MA, USA

Xinyun Zou, Eric O. Scott, Alexander B. Johnson, Kexin Chen, Douglas A. Nitz, Kenneth A. De Jong, Jeffrey L. Krichmar: **Neuroevolution of a recurrent neural network for spatial and working memory in a simulated robotic environment.** GECCO Companion 2021: 289-290, July 10-14, 2021, Lille, France

Adarsha Balaji, Shihao Song, Twisha Titirsha, Anup Das, Jeffrey L. Krichmar, Nikil D. Dutt, James A. Shackleford, Nagarajan Kandasamy, Francky Catthoor: **NeuroXplorer 1.0: An Extensible Framework for Architectural Exploration with Spiking Neural Networks.** ICONS 2021: 10:1-10:9, July 27-29, 2021, Knoxville, TN, USA

Kexin Chen, Alexander B. Johnson, Eric O. Scott, Xinyun Zou, Kenneth A. De Jong, Douglas A. Nitz, Jeffrey L. Krichmar: **Differential Spatial Representations in Hippocampal CA1 and Subiculum Emerge in Evolved Spiking Neural Networks.** IJCNN 2021: 1-8, July 18-22, 2021, Shenzhen, China

Ramtin Afshar, Michael T. Goodrich, Pedro Matias, Martha C. Osegueda: **Parallel Network Mapping Algorithms.** SPAA 2021: 410-413, July 6-8, 2021, Virtual

Publications

Publications

The following papers were published by CECS affiliates from July 2021 through December 2021 (and unreported papers from previous eNews).

Author, Title, Publication — Conference Proceedings

Michael T. Goodrich, Siddharth Gupta, Hadi Khodabandeh, Pedro Matias: **How to Catch Marathon Cheaters: New Approximation Algorithms for Tracking Paths.**WADS 2021: 442-456, July 30-31, 2021, Virtual

Yu-Jye Tung, Ian G. Harris: **Zero Footprint Opaque Predicates: Synthesizing Opaque Predicates from Naturally Occurring Invariants.** DIMVA 2021: 299-318, July 8-9, Virtual

Davide Callegaro, Marco Levorato, Francesco Restuccia: **SeReMAS: Self-Resilient Mobile Autonomous Systems Through Predictive Edge Computing.** SECON 2021: 1-9, July 6-9, Rome, Italy

Nicholas Alonso, Emre Neftci: **Tightening the Biological Constraints on Gradient-Based Predictive Coding.** ICONS 2021: 3:1-3:9, July 27-29, 2021, Knoxville, TN, USA

Hin Wai Lui, Emre Neftci: **Hessian Aware Quantization of Spiking Neural Networks.** ICONS 2021: 12:1-12:5, July 27-29, 2021, Knoxville, TN, USA

Amine Boussik, Wael Ben Messaoud, Smaïl Niar, Abdelmalik Taleb-Ahmed: **Railway Obstacle Detection Using Unsupervised Learning: An Exploratory Study.** IV 2021: 660-667, July 11-17, 2021, Nagoya, Japan

John Thorpe, Yifan Qiao, Jonathan Eyolfson, Shen Teng, Guanzhou Hu, Zhihao Jia, Jinliang Wei, Keval Vora, Ravi Netravali, Miryung Kim, Guoqing Harry Xu: **Dorylus: Affordable, Scalable, and Accurate GNN Training with Distributed CPU Servers and Serverless Threads.** OSDI 2021: 495-514, July 14-16, 2021, Virtual

Publications

Publications

The following papers were published by CECS affiliates from
July 2021 through December 2021 (and unreported papers from previous eNews).

Author, Title, Publication

Journal Publications

Tinoosh Mohsenin, Inna Partin-Vaisband, Houman Homayoun, Jae-Sun Seo, Xin Zhang: **Guest Editorial Cross-Layer Designs, Methodologies, and Systems to Enable Micro AI for On-Device Intelligence.** IEEE J. Emerg. Sel. Topics Circuits Syst. 11(4): 527-531, December, 2021

Fatemeh Davami, Sahar Adabi, Ali Rezaee, Amir Masoud Rahmani: **Distributed scheduling method for multiple workflows with parallelism prediction and DAG prioritizing for time constrained cloud applications.** Comput. Networks 201: 108560, December, 2021

Babak Farhadi, Amir Masoud Rahmani, Parvaneh Asghari, Mehdi Hosseinzadeh: **Friendship selection and management in social internet of things: A systematic review.** Comput. Networks 201: 108568, December, 2021

Mayank Pandey, Rachit Agarwal, Sandeep Kumar Shukla, Nishchal Kumar Verma: **Reputation-based PoS for the Restriction of Illicit Activities on Blockchain: Algorand Usecase.** CoRR abs/2112.11024, December, 2021

Deepesh Chaudhari, Rachit Agarwal, Sandeep Kumar Shukla: **Towards Malicious address identification in Bitcoin.** CoRR abs/2112.11721, December, 2021

Emad Kasaeyan Naeini, Sina Shahhosseini, Anil Kanduri, Pasi Liljeberg, Amir M. Rahmani, Nikil D. Dutt: **AMSER: Adaptive Multi-modal Sensing for Energy Efficient and Resilient eHealth Systems.** CoRR abs/2112.08176, December, 2021

Sanmitra Banerjee, Mahdi Nikdast, Sudeep Pasricha, Krishnendu Chakrabarty: **CHAMP: Coherent Hardware-Aware Magnitude Pruning of Integrated Photonic Neural Networks.** CoRR abs/2112.06098, December, 2021

Sanmitra Banerjee, Mahdi Nikdast, Sudeep Pasricha, Krishnendu Chakrabarty: **Pruning Coherent Integrated Photonic Neural Networks Using the Lottery Ticket Hypothesis.** CoRR abs/2112.07485, December, 2021

Ebadollah Taheri, Sudeep Pasricha, Mahdi Nikdast: **DeFT: A Deadlock-Free and Fault-Tolerant Routing Algorithm for 2.5D Chiplet Networks.** CoRR abs/2112.09234, December, 2021

Evita Bakopoulou, Jiang Zhang, Justin Ley, Konstantinos Psounis, Athina Markopoulou: **Location Leakage in Federated Signal Maps.** CoRR abs/2112.03452, December, 2021

Evita Bakopoulou, Jiang Zhang, Justin Ley, Konstantinos Psounis, Athina Markopoulou: **Location Leakage in Federated Signal Maps.** CoRR abs/2112.03452, December, 2021

Peyman Tehrani, Francesco Restuccia, Marco Levorato: **Federated Deep Reinforcement Learning for the Distributed Control of NextG Wireless Networks.** CoRR abs/2112.03465, December, 2021

Emad Kasaeyan Naeini, Sina Shahhosseini, Anil Kanduri, Pasi Liljeberg, Amir M. Rahmani, Nikil D. Dutt: **AMSER: Adaptive Multi-modal Sensing for Energy Efficient and Resilient eHealth Systems.** CoRR abs/2112.08176, December, 2021

Publications

Publications

The following papers were published by CECS affiliates from July 2021 through December 2021 (and unreported papers from previous eNews).

Author, Title, Publication — Journal Publications

Ali Heydari Gorji, Mahdi Torabzadehkashi, Siavash Rezaei, Hossein Bobarshad, Vladimir Castro Alves, Pai H. Chou: **In-storage Processing of I/O Intensive Applications on Computational Storage Drives.** CoRR abs/2112.12415, December, 2021

Berken Utku Demirel, Islam Abdelsalam Bayoumy, Mohammad Abdullah Al Faruque: **Energy-Efficient Real-Time Heart Monitoring on Edge-Fog-Cloud Internet-of-Medical-Things.** CoRR abs/2112.07901, December, 2021

Sumaya Almanee, Xiafa Wu, Yuqi Huai, Qi Alfred Chen, Joshua Garcia: **scenoRITA: Generating Less-Redundant, Safety-Critical and Motion Sickness-Inducing Scenarios for Autonomous Vehicles.** CoRR abs/2112.09725, December, 2021

Manik Dautta, Abel Jimenez, Kazi Khurshidi Haque Dia, Nafiul Rashid, Mohammad Abdullah Al Faruque, Peter Tseng: **Wireless Qi-Powered, Multinodal and Multisensory Body Area Network for Mobile Health.**IEEE Internet Things J. 8 (9): 7600-7609, November, 2021

Han Wang, Hossein Sayadi, Sai Manoj Pudukotai Dinakarrao, Avesta Sasan, Setareh Rafatirad, Houman Homayoun: **Enabling Micro AI for Securing Edge Devices at Hardware Level.** IEEE J. Emerg. Sel. Topics Circuits Syst. 11 (4): 803-815, November, 2021

Omed Hassan Ahmed, Joan Lu, Qiang Xu, Aram Mahmood Ahmed, Amir Masoud Rahmani, Mehdi Hosseinzadeh: **Using differential evolution and Moth-Flame optimization for scientific workflow scheduling in fog computing.** Appl. Soft Comput. 112: 107744, November, 2021

Venus Mohammadi, Amir Masoud Rahmani, Aso Mohammad Darwesh, Amir Sahafi: **Trust-based Friend Selection Algorithm for navigability in social Internet of Things.** Knowl. Based Syst. 232: 107479, November, 2021

Rahmadi Trimananda, Weiyu Luo, Brian Demsky, Guoqing Harry Xu: **Stateful Dynamic Partial Order Reduction for Model Checking Event-Driven Applications that Do Not Terminate.** CoRR abs/2111.05290, November, 2021

Xiaowu Sun, Yasser Shoukry: **NNSynth: Neural Network Guided Abstraction-Based Controller Synthesis for Stochastic Systems.** CoRR abs/2111.08853, November, 2021

James Ferlez, Haitham Khedr, Yasser Shoukry: **Fast BATLLNN: Fast Box Analysis of Two-Level Lattice Neural Networks.** CoRR abs/2111.09293, November, 2021

Safwen Naimi, Rien van Leeuwen, Wided Souidène, Slim Ben Saoud: **Hybrid BYOL-ViT: Efficient approach to deal with small datasets.** CoRR abs/2111.04845, November, 2021

Elnaz Zafarani-Moattar, Mohammad Reza Kangavari, Amir Masoud Rahmani: **A Comparative Study on Transfer Learning and Distance Metrics in Semantic Clustering over the COVID-19 Tweets.** CoRR abs/2111.08658, November, 2021

Saideep Tiku, Sudeep Pasricha: **Siamese Neural Encoders for Long-Term Indoor Localization with Mobile Devices.** CoRR abs/2112.00654, November, 2021

Publications

Publications

The following papers were published by CECS affiliates from July 2021 through December 2021 (and unreported papers from previous eNews).

Author, Title, Publication — Journal Publications

Yoo Jeong Ha, Soyi Jung, Jae-Hyun Kim, Marco Levorato, Joongheon Kim: **Spatio-Temporal Split Learning for Autonomous Aerial Surveillance using Urban Air Mobility (UAM) Networks.** CoRR abs/2111.11856, November, 2021

Rahmadi Trimananda, Weiyu Luo, Brian Demsky, Guoqing Harry Xu: **Stateful Dynamic Partial Order Reduction for Model Checking Event-Driven Applications that Do Not Terminate.** CoRR abs/2111.05290, November, 2021

Masoomeh Jasemi, Shaahin Hessabi, Nader Bagherzadeh: **Enhancing Reliability of Emerging Memory Technology for Machine Learning Accelerators.** IEEE Trans. Emerg. Top. Comput. 9(4): 2234-2240, October, 2021

Javad Talafy, Farzaneh Zokaee, Hamid R. Zarandi, Nader Bagherzadeh: **A High Performance, Multi-Bit Output Logic -in-Memory Adder.** IEEE Trans. Emerg. Top. Comput. 9(4): 2223-2233, October, 2021

Jurn-Gyu Park, Nikil D. Dutt, Sung-Soo Lim: **An Interpretable Machine Learning Model Enhanced Integrated CPU-GPU DVFS Governor.**ACM Trans. Embed. Comput. Syst. 20(6): 108:1-108:28, October, 2021

Ulkar Ahmadova, Mustafa Mustafayev, Behnam Kiani Kalejahi, Saeed Saeedvand, Amir Masoud Rahmani: **Big data applications on the Internet of Things: A systematic literature review.** Int. J. Commun. Syst. 34(18), October, 2021

Amir Masoud Rahmani, Seyedeh Yasaman Hosseini Mirmahaleh: **A predictor circuit and a delay-aware algorithm for identifying data transfer pattern on NoC-based communication networks.**Microelectron. J. 116: 105250, October, 2021

A. Lee Swindlehurst, Gui Zhou, Rang Liu, Cunhua Pan, Ming Li: **Channel Estimation with Reconfigurable Intelligent Surfaces - A General Framework.** CoRR abs/2110.00553, October, 2021

Venkata Sai Praneeth Karempudi, Febin Sunny, Ishan G. Thakkar, Sai Vineel Reddy Chittamuru, Mahdi Nikdast, Sudeep Pasricha: **Photonic Networks-on-Chip Employing Multilevel Signaling: A Cross-Layer Comparative Study.** CoRR abs/2110.06105, October, 2021

Amir Hosein Afandizadeh Zargari, Marzieh Ashrafiamiri, Minjun Seo, Sai Manoj Pudukotai Dinakarrao, Mohammed E. Fouda, Fadi J. Kurdahi: **CAPTIVE: Constrained Adversarial Perturbations to Thwart IC Reverse Engineering.** CoRR abs/2110.11459, October, 2021

Chongzhou Fang, Han Wang, Najmeh Nazari, Behnam Omidi, Avesta Sasan, Khaled N. Khasawneh, Setareh Rafatirad, Houman Homayoun: **Repttack: Exploiting Cloud Schedulers to Guide Co-Location Attacks.** CoRR abs/2110.00846, October, 2021

Zhuowen Zou, Haleh Alimohamadi, Farhad Imani, Yeseong Kim, Mohsen Imani: **Spiking Hyperdimensional Network: Neuromorphic Models Integrated with Memory-Inspired Framework.** CoRR abs/2110.00214, October, 2021

Mira Hout, Mohammed E. Fouda, Rouwaida Kanj, Ahmed M. Eltawil: **In-memory Multi-valued Associative Processor.** CoRR abs/2110.09643, October, 2021

Mojtaba Taherisadr, Berken Utku Demirel, Mohammad Abdullah Al Faruque, Salma Elmalaki: **Future of Smart Classroom in the Era of Wearable Neurotechnology.** CoRR abs/2110.11475, October, 2021

Publications

The following papers were published by CECS affiliates from July 2021 through December 2021 (and unreported papers from previous eNews).

Author, Title, Publication **Journal Publications**

Shih-Yuan Yu, Arnav Vaibhav Malawade, Mohammad Abdullah Al Faruque: **Multi-Modal Attack Detection for Cyber-Physical Additive Manufacturing.** CoRR abs/2110.02259, October, 2021

Mojtaba Taherisadr, Berken Utku Demirel, Mohammad Abdullah Al Faruque, Salma Elmalaki: **Future of Smart Classroom in the Era of Wearable Neurotechnology.** CoRR abs/2110.11475, October, 2021

Arnav V. Malawade, Shih-Yuan Yu, Brandon Hsu, Deepan Muthirayan, Pramod P. Khargonekar, Mohammad Abdullah Al Faruque: **Spatio-Temporal Scene-Graph Embedding for Autonomous Vehicle Collision Prediction.** CoRR abs/2111.06123, October, 2021

Arnav V. Malawade, Mohanad Odema, Sebastien Lajeunesse-DeGroot, Mohammad Abdullah Al Faruque: **SAGE: A Split-Architecture Methodology for Efficient End-to-End Autonomous Vehicle Control.** ACM Trans. Embed. Comput. Syst. 20(5s): 75:1-75:22 Z, September, 2021

Tianyi Zhang, Minjun Seo, Bryan Donyanavard, Nikil D. Dutt, Fadi J. Kurdahi: **Predicting Failures in Embedded Systems Using Long Short-Term Inference.** IEEE Embed. Syst. Lett. 13(3): 85-89, September, 2021

Adarsha Balaji, Shihao Song, Anup Das, Jeffrey L. Krichmar, Nikil D. Dutt, James A. Shackleford, Nagarajan Kandasamy, Francky Catthoor: **Enabling Resource-Aware Mapping of Spiking Neural Networks via Spatial Decomposition.** IEEE Embed. Syst. Lett. 13(3): 142-145, September, 2021

Biswadip Maity, Saehanseul Yi, Dongjoo Seo, Leming Cheng, Sung-Soo Lim, Jong-Chan Kim, Bryan Donyanavard, Nikil D. Dutt: **Chauffeur: Benchmark Suite for Design and End-to-End Analysis of Self-Driving Vehicles on Embedded Systems.** ACM Trans. Embed. Comput. Syst. 20(5s): 74:1-74:22, September, 2021

Adarsha Balaji, Shihao Song, Anup Das, Jeffrey L. Krichmar, Nikil D. Dutt, James A. Shackleford, Nagarajan Kandasamy, Francky Catthoor: **Enabling Resource-Aware Mapping of Spiking Neural Networks via Spatial Decomposition.** IEEE Embed. Syst. Lett. 13(3): 142-145, September, 2021

Jeffrey L. Krichmar: **Gerald Edelman's Steps Toward a Conscious Artifact.** J. Artif. Intell. Conscious. 8(2): 325-333, September, 2021

Morteza Hosseini, Nitheesh Kumar Manjunath, Bharat Prakash, Arnab Neelim Mazumder, Vandana Chandrareddy, Houman Homayoun, Tinoosh Mohsenin: **Cyclic Sparsely Connected Architectures for Compact Deep Convolutional Neural Networks.** IEEE Trans. Very Large Scale Integr. Syst. 29(10): 1757-1770, September, 2021

Tianyi Zhang, Minjun Seo, Bryan Donyanavard, Nikil D. Dutt, Fadi J. Kurdahi: **Predicting Failures in Embedded Systems Using Long Short-Term Inference.** IEEE Embed. Syst. Lett. 13(3): 85-89, September, 2021

Stephan Adolf, Wolfgang Nebel: **Abstraction NBTI model.** it Inf. Technol. 63(5-6): 299-310, September, 2021

Dharanidhar Dang, Sai Vineel Reddy Chittamuru, Sudeep Pasricha, Rabi N. Mahapatra, Debashis Sahoo: **BPLight-CNN: A Photonics-Based Backpropagation Accelerator for Deep Learning.** ACM J. Emerg. Technol. Comput. Syst. 17(4): 49:1-49:26, September, 2021

Publications

Publications

The following papers were published by CECS affiliates from July 2021 through December 2021 (and unreported papers from previous eNews).

Author, Title, Publication — Journal Publications

Saideep Tiku, Prathmesh Kale, Sudeep Pasricha: **QuickLoc: Adaptive Deep-Learning for Fast Indoor Localization with Mobile Devices.** ACM Trans. Cyber Phys. Syst. 5(4): 44:1-44:30, September, 2021

Febin P. Sunny, Asif Mirza, Mahdi Nikdast, Sudeep Pasricha: **ROBIN: A Robust Optical Binary Neural Network Accelerator.** ACM Trans. Embed. Comput. Syst. 20(5s): 57:1-57:24, September, 2021

Vipin Kumar Kukkala, Sooryaa Vignesh Thiruloga, Sudeep Pasricha: **LATTE: LSTM Self-Attention based Anomaly Detection in E mbedded Automotive Platforms.** ACM Trans. Embed. Comput. Syst. 20(5s): 67:1-67:23, September, 2021

Tong Chen, Jiqiang Liu, He Li, Shuoru Wang, Wenjia Niu, Endong Tong, Liang Chang, Qi Alfred Chen, Gang Li: **Robustness Assessment of Asynchronous Advantage Actor-Critic Based on Dynamic Skewness and Sparseness Computation: A Parallel Computing View.** J. Comput. Sci. Technol. 36(5): 1002-1021, September, 2021

Vaiyee Huynh, Guillaume Burger, Quoc Viet Dang, Raphaël Pelgé, Guilhem Boéris, Jessy W. Grizzle, Aaron D. Ames, Matthieu Masselin: **Versatile Dynamic Motion Generation Framework: Demonstration With a Crutch-Less Exoskeleton on Real-Life Obstacles at the Cybathlon 2020 With a Complete Paraplegic Person.** Frontiers Robotics AI 8: 723780, September, 2021

Soheyla ZakeriKia, Rahman Hajian, Seyed Hossein Erfani, Amir Masoud Rahmani: **Robust and anonymous handover authentication scheme without key escrow problem in vehicular sensor networks.** Wirel. Networks 27(7): 4997-5028, September, 2021

Deliang Chang, Shanshan Hao, Zhou Li, Baojun Liu, Xing Li: **DNSWeight: Quantifying Country-Wise Importance of Domain Name System.** IEEE Access 9: 133240-133257, September, 2021

Sang-Woong Lee, Saqib Ali, Mohammad Sadegh Yousefpoor, Efat Yousefpoor, Pooia Lalbakhsh, Danial Javaheri, Amir Masoud Rahmani, Mehdi Hosseinzadeh: **An Energy-Aware and Predictive Fuzzy Logic-Based Routing Scheme in Flying Ad Hoc Networks (FANETs).** IEEE Access 9: 129977-130005, September, 2021

Yicheng Zhang, Rozhin Yasaei, Hao Chen, Zhou Li, Mohammad Abdullah Al Faruque: **Stealing Neural Network Structure Through Remote FPGA Side-Channel Analysis.** IEEE Trans. Inf. Forensics Secur. 16: 4377-4388, August, 2021

Yicheng Zhang, Rozhin Yasaei, Hao Chen, Zhou Li, Mohammad Abdullah Al Faruque: **Stealing Neural Network Structure Through Remote FPGA Side-Channel Analysis.** IEEE Trans. Inf. Forensics Secur. 16: 4377-4388, August, 2021

Jeffrey L. Krichmar, James Leland Olds, Juan Vicente Sánchez-Andrés, Huajin Tang: **Editorial: Explainable Artificial Intelligence and Neuroscience: Cross-Disciplinary Perspectives.** Frontiers Neurorobotics 15: 731733, August, 2021

Sang-Woong Lee, Haval Mohammed sidqi, Mokhtar Mohammadi, Shima Rashidi, Amir Masoud Rahmani, Mohammad Masdari, Mehdi Hosseinzadeh: **Towards secure intrusion detection systems using deep learning techniques: Comprehensive analysis and review.** J. Netw. Comput. Appl. 187: 103111, August, 2021

Publications

Publications

The following papers were published by CECS affiliates from
July 2021 through December 2021 (and unreported papers from previous eNews).

Author, Title, Publication **Journal Publications**

Hoda Naghibijouybari, Ajaya Neupane, Zhiyun Qian, Nael B. Abu-Ghazaleh: **Side Channel Attacks on GPUs.** IEEE Trans. Dependable Secur. Comput. 18(4): 1950-1961, July, 2021

Zhiqiang Zuo, Kai Wang, Aftab Hussain, Ardalan Amiri Sani, Yiyu Zhang, Shenming Lu, Wensheng Dou, Linzhang Wang, Xuandong Li, Chenxi Wang, Guoqing Harry Xu: **Systemizing Interprocedural Static Analysis of Large-scale Systems Code with Graspan.** ACM Trans. Comput. Syst. 38(1-2): 4:1-4:39, July, 2021

Zhenyuan Li, Qi Alfred Chen, Runqing Yang, Yan Chen, Wei Ruan: **Threat detection and investigation with system-level provenance graphs: A survey.** Comput. Secur. 106: 102282, July, 2021

Nafiul Rashid, Manik Dautta, Peter Tseng, Mohammad Abdullah Al Faruque: **HEAR: Fog-Enabled Energy-Aware Online Human Eating Activity Recognition.** IEEE Internet Things J. 8(2): 860-868, July, 2021

Soheyb Ribouh, Kelvin Phan, Arnav Vaibhav Malawade, Yassin Elhillali, Atika Rivenq, Mohammad Abdullah Al Faruque: **Channel State Information-Based Cryptographic Key Generation for Intelligent Transportation Systems.** IEEE Trans. Intell. Transp. Syst. 22(12): 7496-7507, July, 2021

Seyedeh Yasaman Hosseini Mirmahaleh, Midia Reshadi, Nader Bagherzadeh, Ahmad Khademzadeh: **Data scheduling and placement in deep learning accelerator.** Clust. Comput. 24(4): 3651-3669, July, 2021

Shihao Song, Jui Hanamshet, Adarsha Balaji, Anup Das, Jeffrey L. Krichmar, Nikil D. Dutt, Nagarajan Kandasamy, Francky Catthoor: **Dynamic Reliability Management in Neuromorphic Computing.** ACM J. Emerg. Technol. Comput. Syst. 17(4): 63:1-63:27, July, 2021

Biswadip Maity, Bryan Donyanavard, Anmol Surhonne, Amir M. Rahmani, Andreas Herkersdorf, Nikil D. Dutt:**SEAMS: Self-Optimizing Runtime Manager for Approximate Memory Hierarchies.** ACM Trans. Embed. Comput. Syst. 20 (5): 48:1-48:26, July, 2021

Shihao Song, Jui Hanamshet, Adarsha Balaji, Anup Das, Jeffrey L. Krichmar, Nikil D. Dutt, Nagarajan Kandasamy, Francky Catthoor: **Dynamic Reliability Management in Neuromorphic Computing.** ACM J. Emerg. Technol. Comput. Syst. 17(4): 63:1-63:27, July, 2021

Max Willian Soares Lima, Leonardo Guimarães, Eulanda Miranda dos Santos, Edleno Silva de Moura, Rafael Kohler Costa, Marco Levorato, Horacio A. B. Fernandes de Oliveira: **A Small World Graph Approach for an Efficient Indoor Positioning System.** Sensors 21(15): 5013, July, 2021

Soyi Jung, Joongheon Kim, Marco Levorato, Carlos Cordeiro, Jae-Hyun Kim: **Infrastructure-Assisted on-Driving Experience Sharing for Millimeter-Wave Connected Vehicles.** IEEE Trans. Veh. Technol. 70(8): 7307-7321, July, 2021

Amir Masoud Rahmani, Mokhtar Mohammadi, Shima Rashidi, Jan Lansky, Stanislava Mildeová, Masoumeh Safkhani, Saru Kumari, Mehdi Hosseinzadeh: **Questioning the Security of Three Recent Authentication and Key Agreement Protocols.**IEEE Access 9: 98204-98217, July, 2021

Publications

Publications

The following papers were published by CECS affiliates from July 2021 through December 2021 (and unreported papers from previous eNews).

Author, Title, Publication — Journal Publications

Jan Lansky, Saqib Ali, Mokhtar Mohammadi, Mohammed Kamal Majeed, Sarkhel H. Taher Karim, Shima Rashidi, Mehdi Hosseinzadeh, Amir Masoud Rahmani: **Deep Learning-Based Intrusion Detection Systems: A Systematic Review.** IEEE Access 9: 101574-101599, July, 2021

Mozhdeh Tanha, Mirsaeid Hosseini Shirvani, Amir Masoud Rahmani: **A hybrid meta-heuristic task scheduling algorithm based on genetic and thermodynamic simulated annealing algorithms in cloud computing environments.** Neural Comput. Appl. 33(24): 16951-16984, July, 2021

Abbas Najafizadeh, Afshin Salajegheh, Amir Masoud Rahmani, Amir Sahafi: **Privacy-preserving for the internet of things in multi-objective task scheduling in cloud-fog computing using goal programming approach.** Peer-to-Peer Netw. Appl. 14(6): 3865-3890, July, 2021

Publications

The following papers were published by CECS affiliates from July 2021 through December 2021 (and unreported papers from previous eNews).

Author, Title, Publication **Other Publications**

Xiaowu Sun, Wael Fatnassi, Ulices Santa Cruz, Yasser Shoukry: **Provably Safe Model-Based Meta Reinforcement Learning: An Abstraction-Based Approach.** CoRR abs/2109.01255, September, 2021

James Ferlez, Yasser Shoukry: **Assured Neural Network Architectures for Control and Identification of Nonlinear Systems.** CoRR abs/2109.10298, September, 2021

Febin Sunny, Mahdi Nikdast, Sudeep Pasricha: **SONIC: A Sparse Neural Network Inference Accelerator with Silicon Photonics for Energy-Efficient Deep Learning.** CoRR abs/2109.04459, September, 2021

Sooryaa Vignesh Thiruloga, Vipin Kumar Kukkala, Sudeep Pasricha: **TENET: Temporal CNN with Attention for Anomaly Detection in Automotive Cyber-Physical Systems.** CoRR abs/2109.04565, September, 2021

Jason Kamran Eshraghian, Max Ward, Emre Neftci, Xinxin Wang, Gregor Lenz, Girish Dwivedi, Mohammed Bennamoun, Doo Seok Jeong, Wei D. Lu: **Training Spiking Neural Networks Using Lessons From Deep Learning.** CoRR abs/2109.12894, September, 2021

Kamilya Smagulova, Mohammed E. Fouda, Fadi J. Kurdahi, Khaled N. Salama, Ahmed M. Eltawil: **Resistive Neural Hardware Accelerators.** CoRR abs/2109.03934, September, 2021

Ali Shaib, Mohamad H. Naim, Mohammed E. Fouda, Rouwaida Kanj, Fadi J. Kurdahi: **Efficient Noise Mitigation Technique for Quantum Computing.** CoRR abs/2109.05136, September, 2021

Shaoshan Liu, Yuhao Zhu, Bo Yu, Jean-Luc Gaudiot, Guang R. Gao: **The Promise of Dataflow Architectures in the Design of Processing Systems for Autonomous Machines.** CoRR abs/2109.07047, September, 2021

Kamilya Smagulova, Mohammed E. Fouda, Fadi J. Kurdahi, Khaled N. Salama, Ahmed M. Eltawil: **Resistive Neural Hardware Accelerators.** CoRR abs/2109.03934, September, 2021

Yuxin (Myles) Liu, Yoshimichi Nakatsuka, Ardalan Amiri Sani, Sharad Agarwal, Gene Tsudik: **Vronicle: A System for Producing Videos with Verifiable Provenance.** CoRR abs/2109.12712, September, 2021

Arnav Vaibhav Malawade, Shih-Yuan Yu, Brandon Hsu, Harsimrat Kaeley, Anurag Karra, Mohammad Abdullah Al Faruque: **roadscene2vec: A Tool for Extracting and Embedding Road Scene-Graphs.** CoRR abs/2109.01183, September, 2021

Trier Mortlock, Deepan Muthirayan, Shih-Yuan Yu, Pramod P. Khargonekar, Mohammad Abdullah Al Faruque: **Graph Learning for Cognitive Digital Twins in Manufacturing Systems.** CoRR abs/2109.08632, September, 2021

Won Park, Nan Liu, Qi Alfred Chen, Z. Morley Mao: **Sensor Adversarial Traits: Analyzing Robustness of 3D Object Detection Sensor Fusion Models.** CoRR abs/2109.06363, September, 2021

Nisha Panwar, Shantanu Sharma, Guoxi Wang, Sharad Mehrotra, Nalini Venkatasubramanian, Mamadou H. Diallo, Ardalan Amiri Sani: **IoT Notary: Attestable Sensor Data Capture in IoT Environments.** CoRR abs/2108.02293, August, 2021

Iknoor Singh, Carolina Scarton, Kalina Bontcheva: **Multistage BiCross Encoder: Team GATE Entry for MLIA Multilingual Semantic Search Task 2.** CoRR abs/2101.03013, August, 2021

Publications

Publications

The following papers were published by CECS affiliates from July 2021 through December 2021 (and unreported papers from previous eNews).

Author, Title, Publication

Other Publications

Ali Tazarv, Sina Labbaf, Amir M. Rahmani, Nikil D. Dutt, Marco Levorato: **Data Collection and Labeling of Real-Time IoT-Enabled Bio-Signals in Everyday Settings for Mental Health Improvement.** CoRR abs/2108.01169, August, 2021

Renjie Xie, Wei Xu, Yanzhi Chen, Jiabao Yu, Aiqun Hu, Derrick Wing Kwan Ng, A. Lee Swindlehurst: **A Generalizable Model-and-Data Driven Approach for Open-Set RFF Authentication.** CoRR abs/2108.04436, August, 2021

Nisha Panwar, Shantanu Sharma, Guoxi Wang, Sharad Mehrotra, Nalini Venkatasubramanian, Mamadou H. Diallo, Ardalan Amiri Sani: **IoT Notary: Attestable Sensor Data Capture in IoT Environments.** CoRR abs/2108.02293, August, 2021

Nafiul Rashid, Luke Chen, Manik Dautta, Abel Jimenez, Peter Tseng, Mohammad Abdullah Al Faruque: **Feature Augmented Hybrid CNN for Stress Recognition Using Wrist-based Photoplethysmography Sensor.** CoRR abs/2108.03166, August, 2021

Banwari Lal, Rachit Agarwal, Sandeep Kumar Shukla: **Understanding Money Trails of Suspicious Activities in a cryptocurrency-based Blockchain.** CoRR abs/2108.11818, August, 2021

Ali Tazarv, Sina Labbaf, Amir M. Rahmani, Nikil D. Dutt, Marco Levorato: **Data Collection and Labeling of Real-Time IoT-Enabled Bio-Signals in Everyday Settings for Mental Health Improvement.** CoRR abs/2108.01169, August, 2021

Yoshitomo Matsubara, Ruihan Yang, Marco Levorato, Stephan Mandt: **Supervised Compression for Resource-constrained Edge Computing Systems.** CoRR abs/2108.11898, August, 2021

Ali Tazarv, Sina Labbaf, Amir M. Rahmani, Nikil D. Dutt, Marco Levorato: **Data Collection and Labeling of Real-Time IoT-Enabled Bio-Signals in Everyday Settings for Mental Health Improvement.** CoRR abs/2108.01169, August, 2021

Nafiul Rashid, Luke Chen, Manik Dautta, Abel Jimenez, Peter Tseng, Mohammad Abdullah Al Faruque: **Feature Augmented Hybrid CNN for Stress Recognition Using Wrist-based Photoplethysmography Sensor.** CoRR abs/2108.03166, August, 2021

Nisha Panwar, Shantanu Sharma, Guoxi Wang, Sharad Mehrotra, Nalini Venkatasubramanian, Mamadou H. Diallo, Ardalan Amiri Sani: **IoT Notary: Attestable Sensor Data Capture in IoT Environments.** CoRR abs/2108.02293, August, 2021

Bowen Tang, Chenggang Wu, Zhe Wang, Lichen Jia, Pen-Chung Yew, Yueqiang Cheng, Yinqian Zhang, Chenxi Wang, Guoqing Harry Xu: **SpecBox: A Label-Based Transparent Speculation Scheme Against Transient Execution Attacks.** CoRR abs/2107.08367, July, 2021

Tiago Mück, Bryan Donyanavard, Biswadip Maity, Kasra Moazzemi, Nikil D. Dutt: **MARS: Middleware for Adaptive Reflective Computer Systems.** CoRR abs/2107.11417, July, 2021

Rozhin Yasaei, Shih-Yuan Yu, Emad Kasaeyan Naeini, Mohammad Abdullah Al Faruque: **GNN4IP: Graph Neural Network for Hardware Intellectual Property Piracy Detection.** CoRR abs/2107.09130, July, 2021

Publications

Publications

The following papers were published by CECS affiliates from
July 2021 through December 2021 (and unreported papers from previous eNews).

Author, Title, Publication — Other Publications

Mohanad Odema, Nafiul Rashid, Berken Utku Demirel, Mohammad Abdullah Al Faruque: **LENS: Layer Distribution Enabled Neural Architecture Search in Edge-Cloud Hierarchies.** CoRR abs/2107.09309, July, 2021

Tuo Zhou, Shih-Yuan Yu, Matthew Michaels, Fangzhou Du, Lawrence Kulinsky, Mohammad Abdullah Al Faruque: **Establishing Digital Recognition and Identification of Microscopic Objects for Implementation of Artificial Intelligence (AI) Guided Microassembly.** CoRR abs/2107.10823, July, 2021

Arnav V. Malawade, Mohanad Odema, Sebastien Lajeunesse-DeGroot, Mohammad Abdullah Al Faruque: **SAGE: A Split-Architecture Methodology for Efficient End-to-End Autonomous Vehicle Control.** CoRR abs/2107.10895, July, 2021

Shih-Yuan Yu, Rozhin Yasaei, Qingrong Zhou, Tommy Nguyen, Mohammad Abdullah Al Faruque: **HW2VEC: A Graph Learning Tool for Automating Hardware Security.** CoRR abs/2107.12328, July, 2021

Ali Tazarv, Sina Labbaf, Stephanie M. Reich, Nikil D. Dutt, Amir M. Rahmani, Marco Levorato: **Personalized Stress Monitoring using Wearable Sensors in Everyday Settings.** CoRR abs/2108.00144, July, 2021

Liping Wang, Saideep Tiku, Sudeep Pasricha: **CHISEL: Compression-Aware High-Accuracy Embedded Indoor Localization with Deep Learning.** CoRR abs/2107.01192, July, 2021

Febin P. Sunny, Asif Mirza, Mahdi Nikdast, Sudeep Pasricha: **ROBIN: A Robust Optical Binary Neural Network Accelerator.** CoRR abs/2107.05530, July, 2021

Vipin Kumar Kukkala, Sooryaa Vignesh Thiruloga, Sudeep Pasricha: **LATTE: LSTM Self-Attention based Anomaly Detection in Embedded Automotive Platforms.** CoRR abs/2107.05561, July, 2021

Ali Tazarv, Marco Levorato: **A Deep Learning Approach to Predict Blood Pressure from PPG Signals.** CoRR abs/2108.00099, July, 2021

Ali Tazarv, Sina Labbaf, Stephanie M. Reich, Nikil D. Dutt, Amir M. Rahmani, Marco Levorato: **Personalized Stress Monitoring using Wearable Sensors in Everyday Settings.** CoRR abs/2108.00144, July, 2021

Tiago Mück, Bryan Donyanavard, Biswadip Maity, Kasra Moazzemi, Nikil D. Dutt: **MARS: Middleware for Adaptive Reflective Computer Systems.** CoRR abs/2107.11417, July, 2021

Yasamin Moghaddas, Tommy Nguyen, Shih-Yuan Yu, Rozhin Yasaei, Mohammad Abdullah Al Faruque: **Technical Report for HW2VEC - A Graph Learning Tool for Automating Hardware Security.** CoRR abs/2108.00078, July, 2021

Takami Sato, Qi Alfred Chen: **On Robustness of Lane Detection Models to Physical-World Adversarial Attacks in Autonomous Driving.** CoRR abs/2107.02488, July, 2021

CECS—*promoting creativity and pursuing discovery!*

Center for Embedded and Cyber-Physical Systems, University of California, Irvine

***CECS** Mission Statement:*

To conduct leading-edge interdisciplinary research in embedded systems emphasizing automotive, communications, and medical applications, and to promote technology and knowledge transfer for the benefit of the individual and society.

CECS eNews
Center for Embedded and Cyber-Physical Systems
3211 Engineering Hall
University of California, Irvine
Email:
enews@cecs.uci.edu