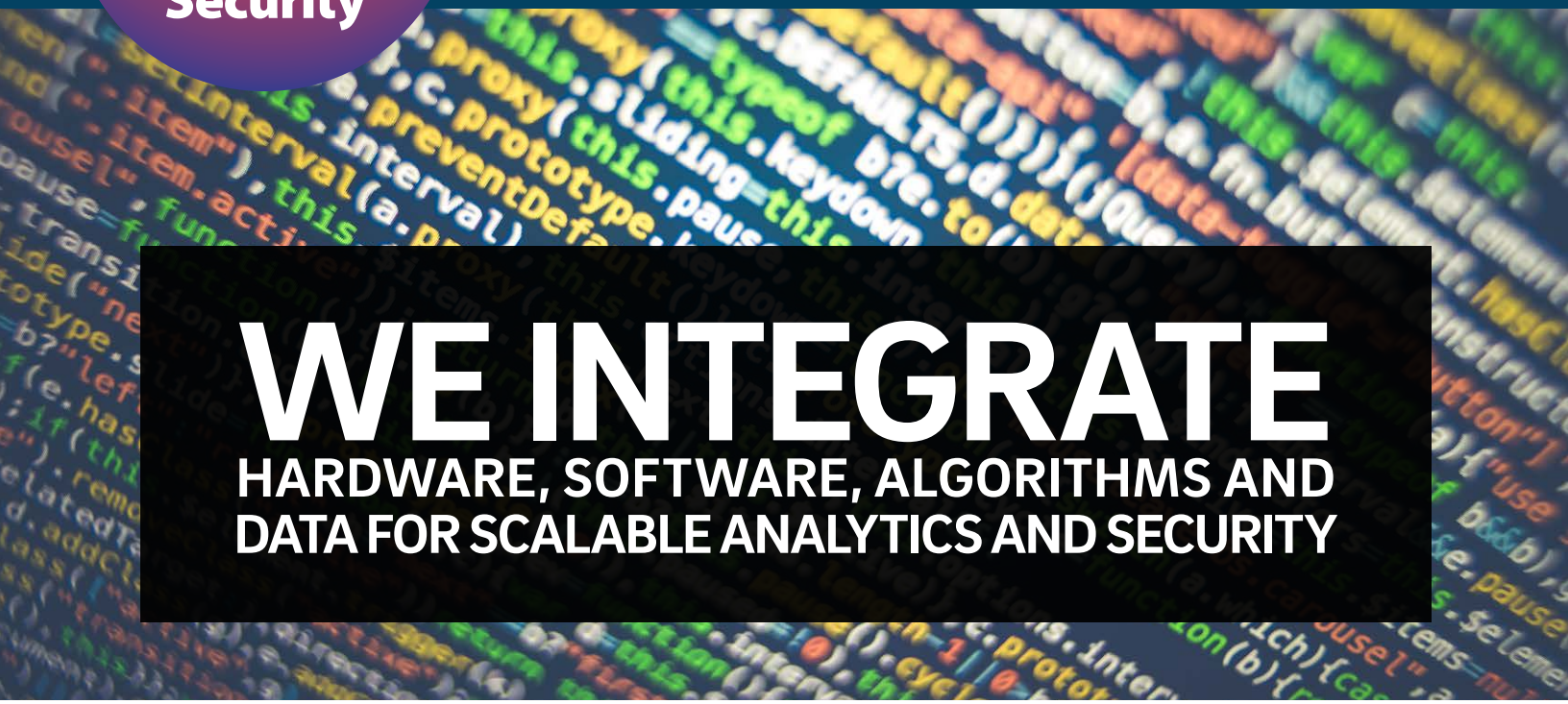
Center for
Machine-Integrated Computing & Security

UC San Diego
JACOBS SCHOOL OF ENGINEERING



WE INTEGRATE
HARDWARE, SOFTWARE, ALGORITHMS AND DATA FOR SCALABLE ANALYTICS AND SECURITY

OUR SOLUTIONS ARE AUTOMATED **AND** CUSTOMIZED

HARDWARE ACCELERATION + SYSTEM-OPTIMIZATION ENGINES

REAL-TIME DATA ANALYTICS

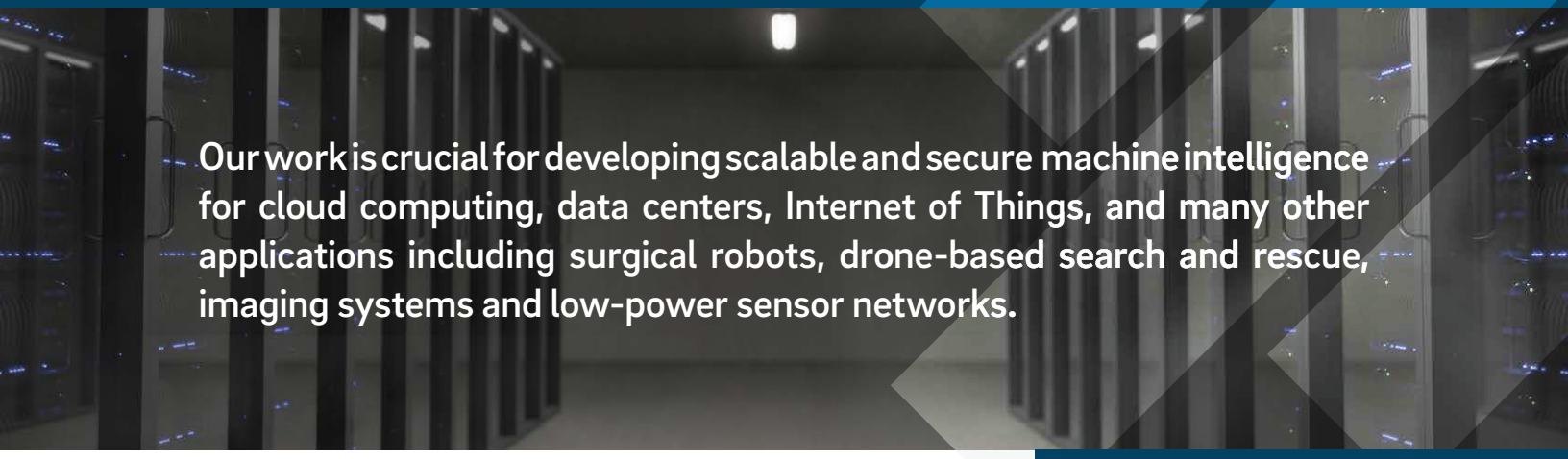
Hardware, software and algorithm co-design for real-time data analytics. Our customized performance optimization engine is automated and works across platforms, from low-power sensors to data centers and the cloud. Our solutions integrate adaptive data collection processes with training, learning, and inference in real-time and streaming applications.

PARADIGM SHIFT IN DEEP LEARNING

Automated acceleration and adaptive retraining of deep learning. Our framework allows for training of deep learning networks that are platform independent, and scale from sensors to mobile to data centers. We introduced a paradigm shift when we built and demonstrated the first training of deep learning on mobile (edge) devices.

SECURITY AND PRIVACY FOR CYBER-PHYSICAL SYSTEMS

To secure cyber-physical systems, we fully consider hardware, software, algorithms and data – and their isolation and interactions. We offer new approaches to security and privacy. Safe machine learning / defense against adversarial attacks, secure embedded medical devices, and privacy-preserving computing (DNA, learning, biometrics) are examples.



Our work is crucial for developing scalable and secure machine intelligence for cloud computing, data centers, Internet of Things, and many other applications including surgical robots, drone-based search and rescue, imaging systems and low-power sensor networks.

CENTER LEADERSHIP

Farinaz Koushanfar

Center Co-Director
Electrical & Computer Engineering Professor

Farinaz Koushanfar's research contributions include:

Development of novel scalable domain-specific machine learning solutions.

Creation of the first scalable methodology for computing on private (encrypted) data using secure function evaluation. Koushanfar reported the first secure general purpose processor for leakage-resilient cryptography.

Invention of hardware metering, the first suite of methods for tracing chips post fabrication.

Devising the first set of comprehensive methods and metrics to characterize the safety of deep learning models. Her team conceived the first methodology which thwarts all known adversarial machine learning attacks.

Tara Javidi

Center Co-Director
Electrical & Computer Engineering Professor

Tara Javidi's research covers broad theoretical questions as well as practical solutions for information acquisition, processing, and communication. Current projects include:

Information acquisition-utilization and controlled sensing. In addition to developing the theory, her group has applied the theory in diverse settings from flight optimization for drones to feature selection in computer vision.

Stochastic control and optimization of networks. The focus is on optimization of autonomous, collaborative, cyber-physical platforms like cars and drones as distributed sensing platforms or wireless infrastructure.

Active machine learning with imperfect labelers. In collaboration with K. Chaudhuri, her team has developed the first fully adaptive scheme to learn from consistently imperfect labels.

BENEFITS OF PARTNERSHIP

The Center provides industry partners with a coordinated research environment in which technical challenges are tackled collaboratively.

- **Seat on the Center Advisory Board**
- **Influence and advise industry-relevant research priorities**
- **Recruit our top students**
- **Access to multidisciplinary researchers with shared focus**
- **Embed a Visiting Industry Fellow in our labs**
- **Industry-faculty-student research teams**
- **Fast-track research agreements**
- **Access to lab-to-market business and technology accelerators**
- **Invitations to Research Summits**

CONNECT WITH US

Farinaz Koushanfar
Electrical & Computer Engineering Professor
fkoushanfar@eng.ucsd.edu
+1 (619) 246-0251

Tara Javidi
Electrical & Computer Engineering Professor
tjavidi@eng.ucsd.edu
+1 (858) 822-4924

Lon McPhail
Director for Corporate Research Partnerships
lmcphail@eng.ucsd.edu
+1 (619) 840-7600

v 1712