From Data Management to Data Trust: Securing AI-Driven Construction Systems in the Physical World

Yu Chen, Ph.D.

Bio

Dr. Yu Chen is a Professor in the Department of Electrical and Computer Engineering at Binghamton University (SUNY), where he directs the Ubiquitous Smart & Sustainable Computing (US2C) Lab and serves as Associate Director of the Center for Information Assurance and Cybersecurity (CIAC). He earned his Ph.D. in Electrical Engineering from the University of Southern California in 2006, studying under Professor Kai Hwang. His research centers on trust, security, and privacy in computer networks, including edge-fog-cloud computing, the Internet of Things (IoT), and their applications in smart cities and intelligent surveillance systems. Dr. Chen has authored or co-authored more than 200 scientific papers in refereed journals, conferences, and book chapters. His work has been supported by the National Science Foundation, Department of Defense, Air Force Office of Scientific Research, Air Force Research Laboratory, New York State, and industry partners. He is a Senior Member of the IEEE Computer Society and Communications Society, and a member of ACM and SPIE.

Abstract

The construction engineering ecosystem is rapidly transitioning from document-centric workflows to AI-driven, data-centric systems that sense, analyze, decide, and act in the physical world. Drones, vision systems, digital twins, autonomous equipment, and sensor-rich job sites now rely on continuous streams of multimodal data to support safety monitoring, quality assurance, scheduling, and lifecycle asset management. In this environment, research data management cannot be treated as a back-end compliance or archival function. Instead, it becomes a foundational trust layer: if data feeding AI-enabled construction systems is incomplete, manipulated, misattributed, or decoupled from physical reality, downstream decisions may be unsafe, misleading, or irreversible.

This keynote argues for a paradigm shift from traditional data management to data trust in construction engineering research and practice. Drawing from advances in cyber-physical systems security, trustworthy AI, and physical-reality grounding, the talk examines emerging threats to construction data pipelines, including sensor spoofing, synthetic and AI-generated content, data poisoning, and provenance breaks across long-lived infrastructure projects. It outlines design principles for adversarial-aware research data management that integrate provenance, integrity, physical anchoring, and post-hoc forensics directly into data collection and curation workflows. By reframing construction data as an active component of safety-critical AI systems rather than a passive research artifact, this keynote highlights new research opportunities at the intersection of data management, AI, and cyber-physical trust, and challenges the community to rethink how data must be managed when it directly shapes decisions in the built environment.