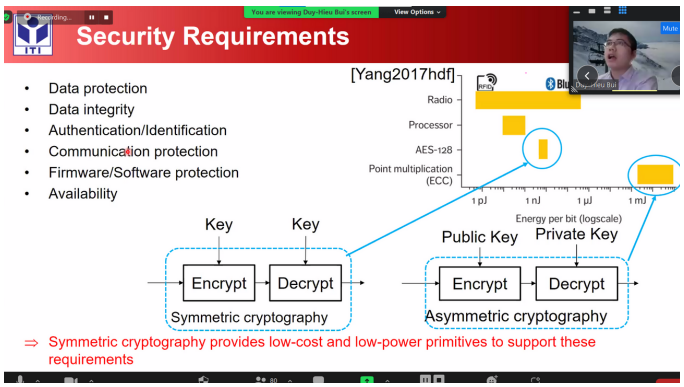
VIỆN CÔNG NGHỆ THÔNG TIN TỔ CHỨC HỘI THẢO KHOA HỌC

"Mạng Internet vạn vật (IoT): một số vấn đề về bảo mật và trí tuệ nhân tạo"



Ngày 10/9/2021, Viện Công nghệ Thông tin đã tổ chức Hội thảo khoa học với chủ đề "Mạng Internet vạn vật (IoT): một số vấn đề về bảo mật và trí tuệ nhân tạo" do PGS.TS. Trần Xuân Tú chủ trì. Hội thảo đã thu hút gần 100 nhà khoa học, chuyên gia và kỹ sư công nghệ đến từ các trường đại học, viện nghiên cứu và doanh nghiệp công nghệ tham dự. Hội nghị đã nghe 03 báo cáo của các chuyên gia đến từ Học viện Kỹ thuật Quân sự và Viện Công nghệ Thông tin: Báo cáo thứ nhất "Các cơ hội và thách thức trong thiết kế và phát triển phần cứng an toàn và giải pháp an toàn phần cứng cho các thiết bị IoT có công suất tiêu thụ siêu thấp" do TS. Bùi Duy Hiếu, Phòng Công nghệ mạng và truyền thông, Viện Công nghệ Thông tin trình bày. Bài báo cáo đã tổng quan các xu hướng công nghệ và các nghiên cứu mới liên quan đến việc xây dựng và lựa chọn giải pháp triển khai các thuật toán mã hóa bảo mật phù hợp cho các thiết bị IoT tiêu thụ điện năng siêu thấp và các nghiên cứu phát triển hiện tại của nhóm nghiên cứu về giải pháp phần cứng bảo mật cũng như nền tảng đánh giá ước lượng mức độ bảo mật phần cứng do nhóm đề xuất dựa trên các công cụ ước lượng công suất tiêu thụ chuyên dụng. Báo cáo thứ hai về "Phân tích kênh bên dựa vào học máy và nhận biết phần cứng gián điệp" do PGS.TS. Hoàng Văn Phúc, Viện Tích hợp, Học viện Kỹ thuật Quân sự trình bày. Bài trình bày của PGS.TS. Hoàng Văn Phúc cũng đề cập đến các giải pháp ứng dụng học máy trong bảo mật phần cứng cho các hệ thống IoT an toàn với trọng tâm là phân tích kênh bên dựa trên học máy và phát hiện phần cứng gián điệp. Báo cáo thứ ba đề cập đến "Kiến trúc phần cứng cho mạng nơ-ron xung điện (Deep Spiking Neural Networks) và một số kết quả nghiên cứu" do ThS. Nguyễn Duy Anh trình bày. Nhóm đã đề xuất một phương pháp huấn luyện thân thiện với phần cứng cho DSNN cho phép các trọng số được giới hạn ở định dạng bậc ba, nhờ đó giảm được không gian bộ nhớ và mức độ tiêu thụ năng lượng. Mô phỏng phần mềm trên bộ dữ liệu MNIST và CIFAR10 cho thấy phương pháp huấn luyện có thể đạt độ chính xác 97% đối với MNIST (mạng kết nối đầy đủ 3 lớp) và 89,71% đối với CIFAR10 (VGG16).