Innovative AI technologies for sophisticated integration of cyber and physical world

Research of Hardware Security on Edge AI Hardware

Project Leader : Takeshi Fujino
Professor, Department of Electronic and Computer Engineering, Ritsumeikan University

R&D Team : Information Technology R&D Center, Mitsubishi Electric Corporation

Summary :

"Edge AI" is getting more important from the viewpoint of real-time operation and privacy protection. On the other hand, "edge AI" on the physical space has more security vulnerability than "cloud AI" on the cyberspace, because attackers can physically access AI processing hardware. For example, AI models (DNN network structure and weight parameters) can be revealed by memory-bus tapping or side-channel attack exploiting power consumption or electromagnetic waves. Malfunction can also be induced by fault-injection attack. In this research, hardware security threats on "edge AI" are comprehensively analyzed, and countermeasures are studied to prevent these attacks.

<Security Countermeasures> (1) Data encryption of AI models against memory bus tapping. (2) Elimination of Side-channel leaks and increase of fault tolerance on AI processing hardware. (3) Integrity check and/or encryption from CMOS image sensor data.

<Benefits> (1) Protection of intellectual property on AI models. (2) Prevention of AI-specific malfunctions (such as Adversarial Examples). (3) Privacy protection of image data used for AI learning or inference.