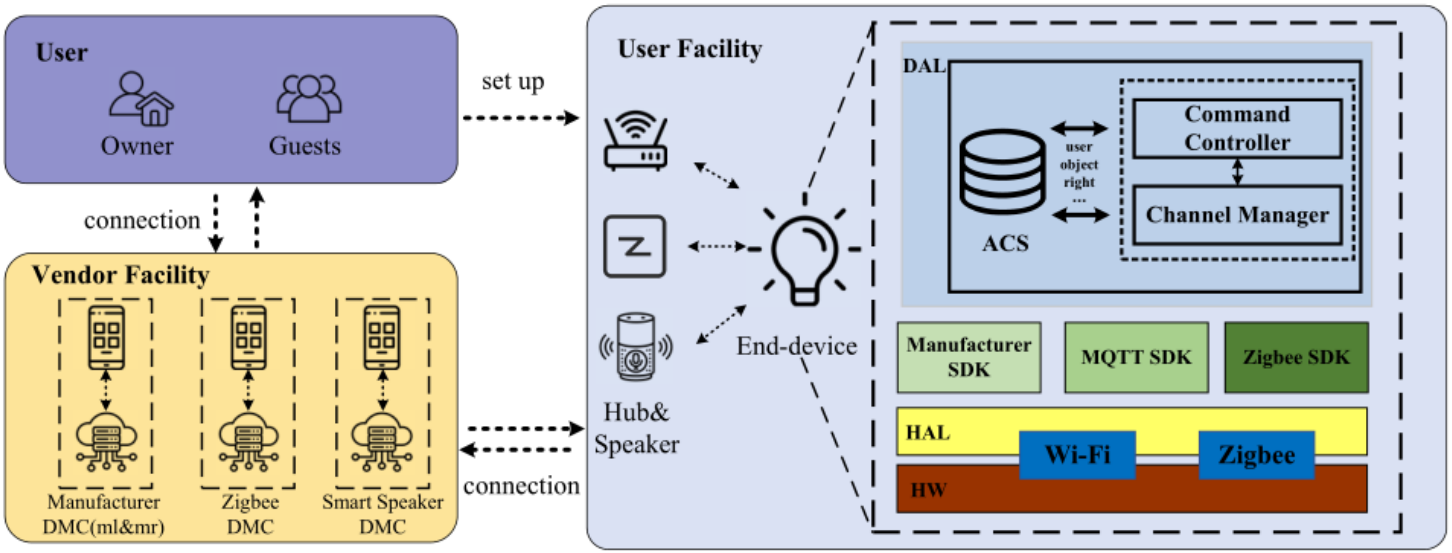
DMCGuard: Risky Perils and Fine-Grained Control on IoT Multiple Device Management Channels

Bin YUAN, Kaimin ZHENG, Yan JIA, Jiajun REN, Kunming WANG, Shengjiu SHI, Deqing ZOU, Hai JIN

Frontiers of Computer Science, DOI: 10.1007/s11704-024-40143-0

Problems & Ideas

- Problems of multi-user Device Management Channels (DMCs):
  - Lack of fine-grained attribute management among multi-DMC IoT can lead to permission abuse and privacy leakage.
  - Existing solutions inadequately address limitations and security concerns in multi-user DMCs access control.
- Ideas: DMCGuard, a novel multi-DMC IoT access framework, provides fine-grained control with security policies.



DMCGuard access control framework involves four main components: the end device, the IoT hubs, the IoT cloud servers and the user mobile apps, which work together to establish an IoT ecosystem.

Main Contributions

- Contributions:
  - A detailed analysis of the manufacturer local DMCs, shedding light on previously overlooked security issues;
  - A novel model, MDUCON, is provided to tackle the security challenges associated with managing multiple DMCs;
  - A new solution, DMCGuard, is designed to provide fine-grained and multi-DMC access control.

Evaluation items	*CGuard* [5]	*DMCGuard*
Multi-DMC management	✓	✓
Multi-user management	×	✓
Multi-attribute management	×	✓
Local DMC support	×	✓
Extra storage overhead	2.91 MB	746 KB

Compared to CGuard, DMCGuard offers advanced, fine-grained access control, using criteria like user IDs, device attributes, and DMCs for authentication.