BÀI #20 - BẢO MẬT & QUYỀN RIÊNG TƯ CỦA IoT

TS. HOÀNG SỸ TƯƠNG

BÀI #20 - BẢO MẬT & QUYỀN RIÊNG TƯ CỦA IOT

- IoT là gì? ...WoT là gì?
  - IoT # internet, WoT # web
- ví dụ về các vấn đề tiềm ẩn về bảo mật và quyền riêng tư trong các tình huống sử dụng IoT hiện tại và tương lai gần
- những thay đổi về kiến trúc có thể giải quyết những vấn đề này

INTERNET VẠN VẬT LÀ...?

- Chúng ta quan tâm đến những thứ gì khi kết nối internet? máy tính, máy tính xách tay và điện thoại di động là tất cả mọi thứ...liệu nó đã tồn tại được 40 năm chưa?
- Nếu tôi gắn chip wi-fi vào cảm biến và dán cảm biến lên tường, có phải tôi vừa tạo ra internet of things không?
- Khi bộ điều nhiệt nest của tôi điều khiển máy sưởi của tôi bằng cách sử dụng dữ liệu từ đám mây, đó có phải là internet vạn vật không?

Câu nói IoT yêu thích của tôi: *"đó không phải là internet của **(OF)** vạn vật, đó là internet với **(WITH)** vạn vật."*

VẬY, INTERNET VẠN VẬT LÀ...?

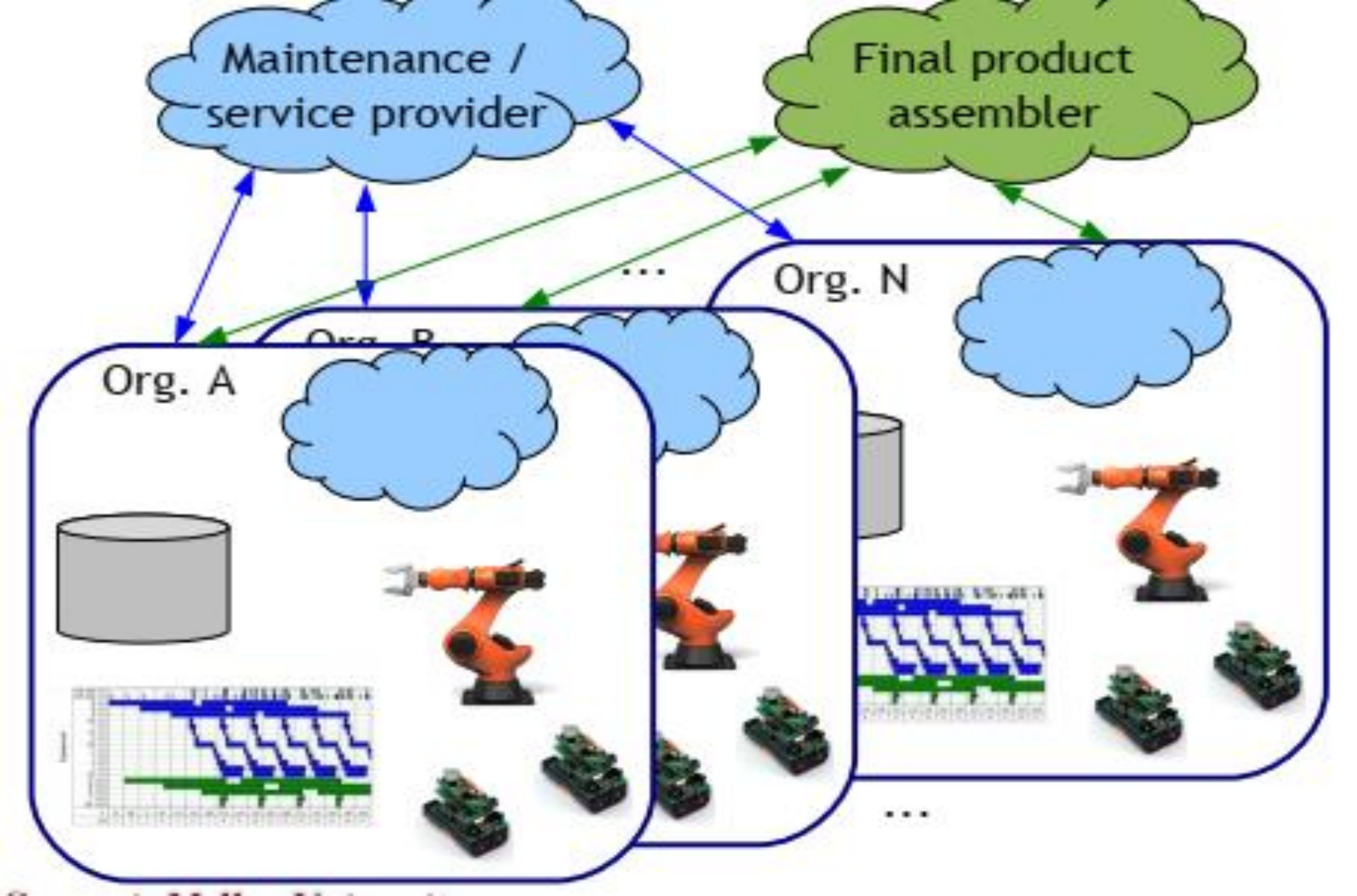
- Nó phức tạp lắm - mọi người đều có định nghĩa riêng của họ.
- Hầu hết là do:

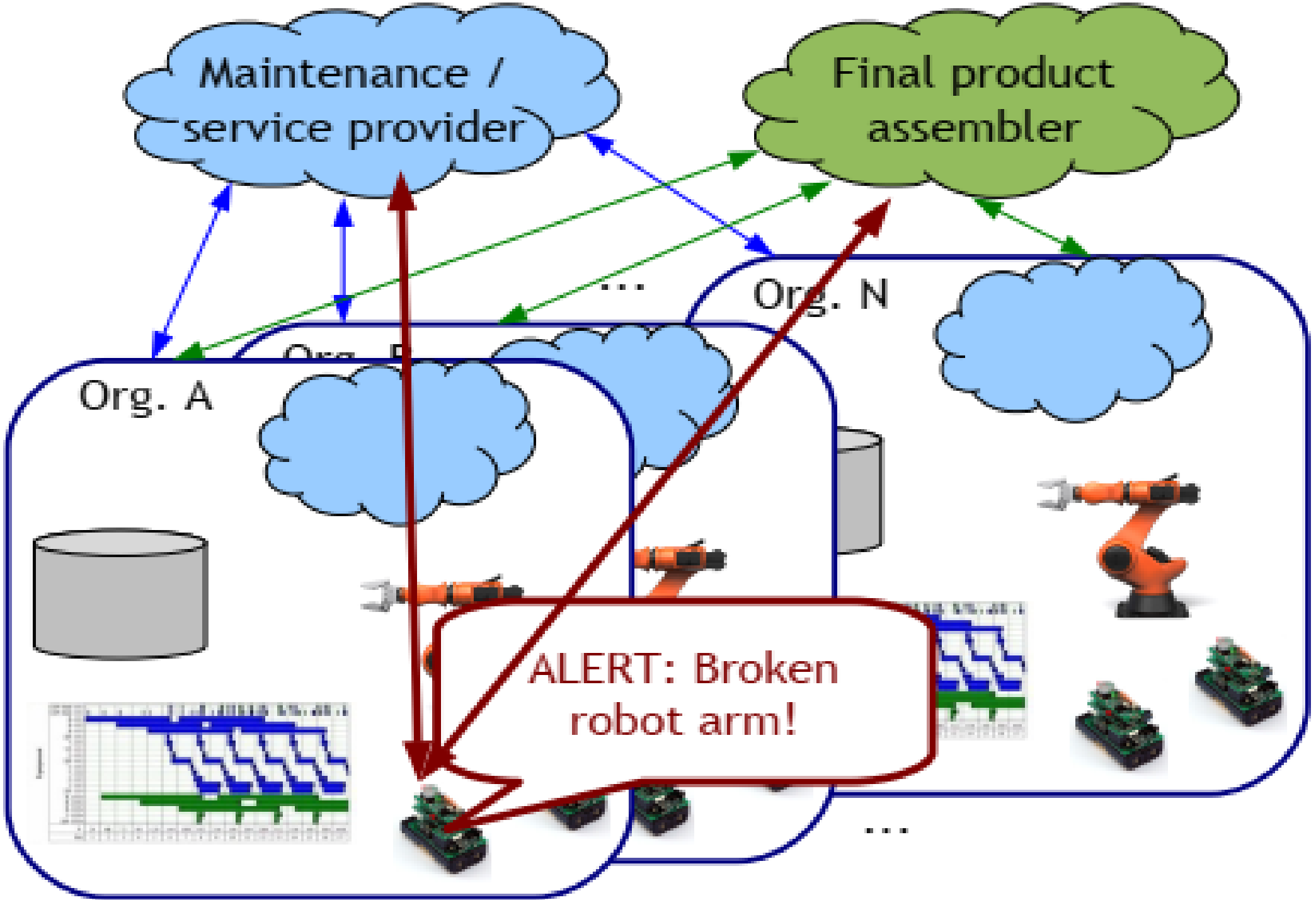
Cho phép những thứ được nhúng cộng tác để cung cấp một số loại dịch vụ cho người dùng, ứng dụng hoặc những thứ khác

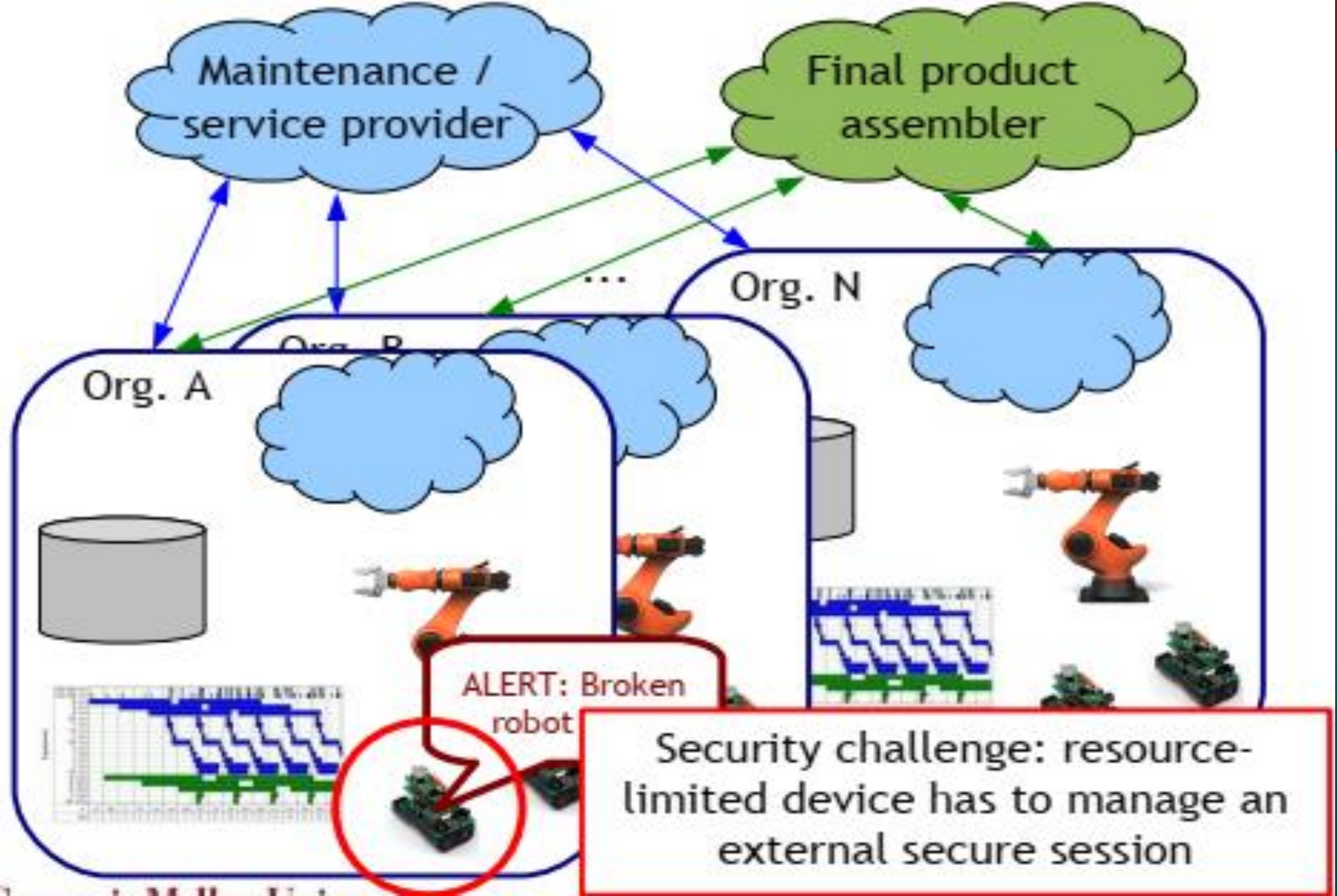
Các ứng dụng có thể lấy dữ liệu từ một số thứ, xử lý dữ liệu bằng những thứ khác, đưa ra quyết định bằng những thứ khác và tác động đến thế giới thực bằng những thứ khác

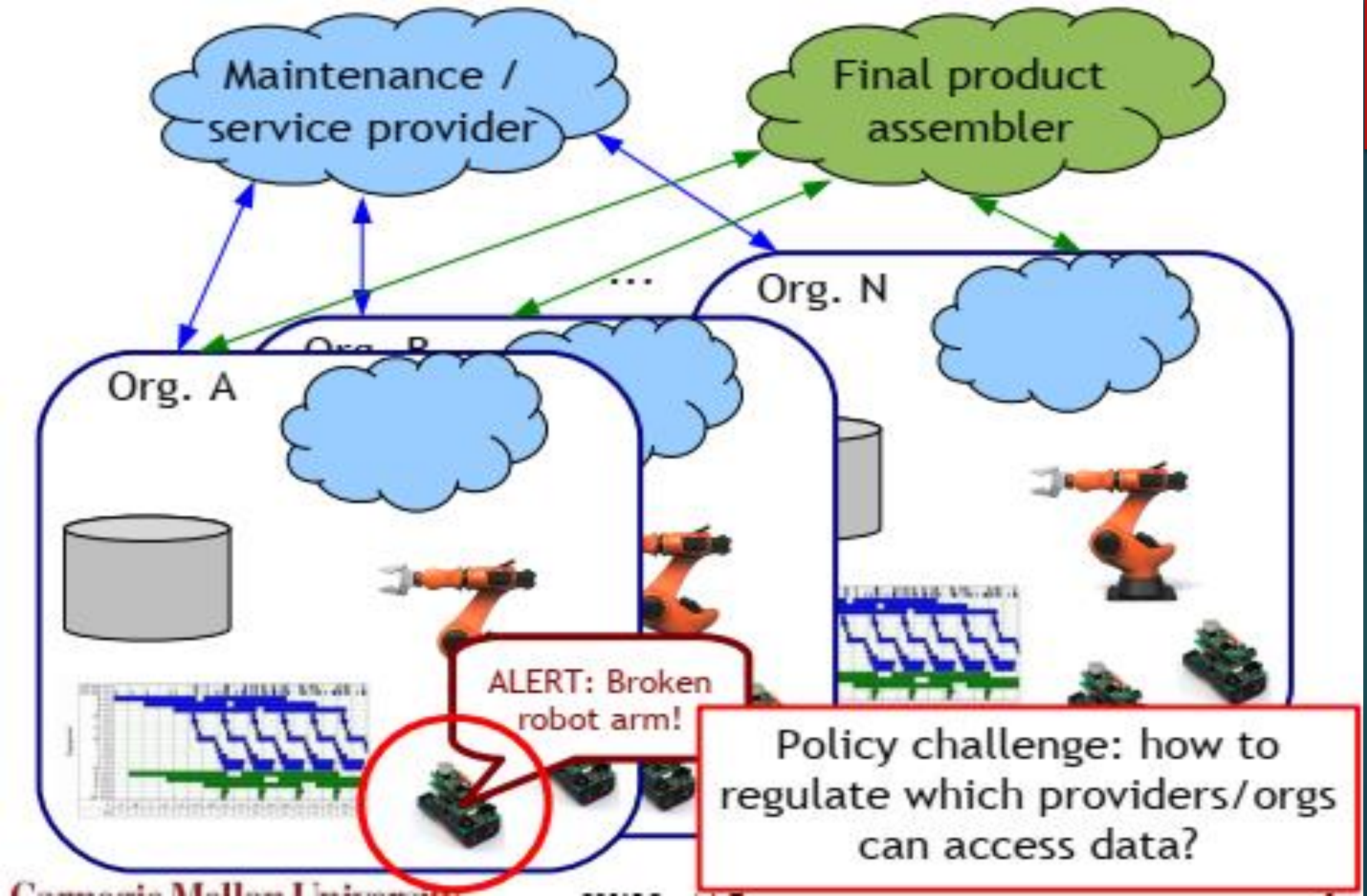
- Nhiều thứ trong số này là không dây

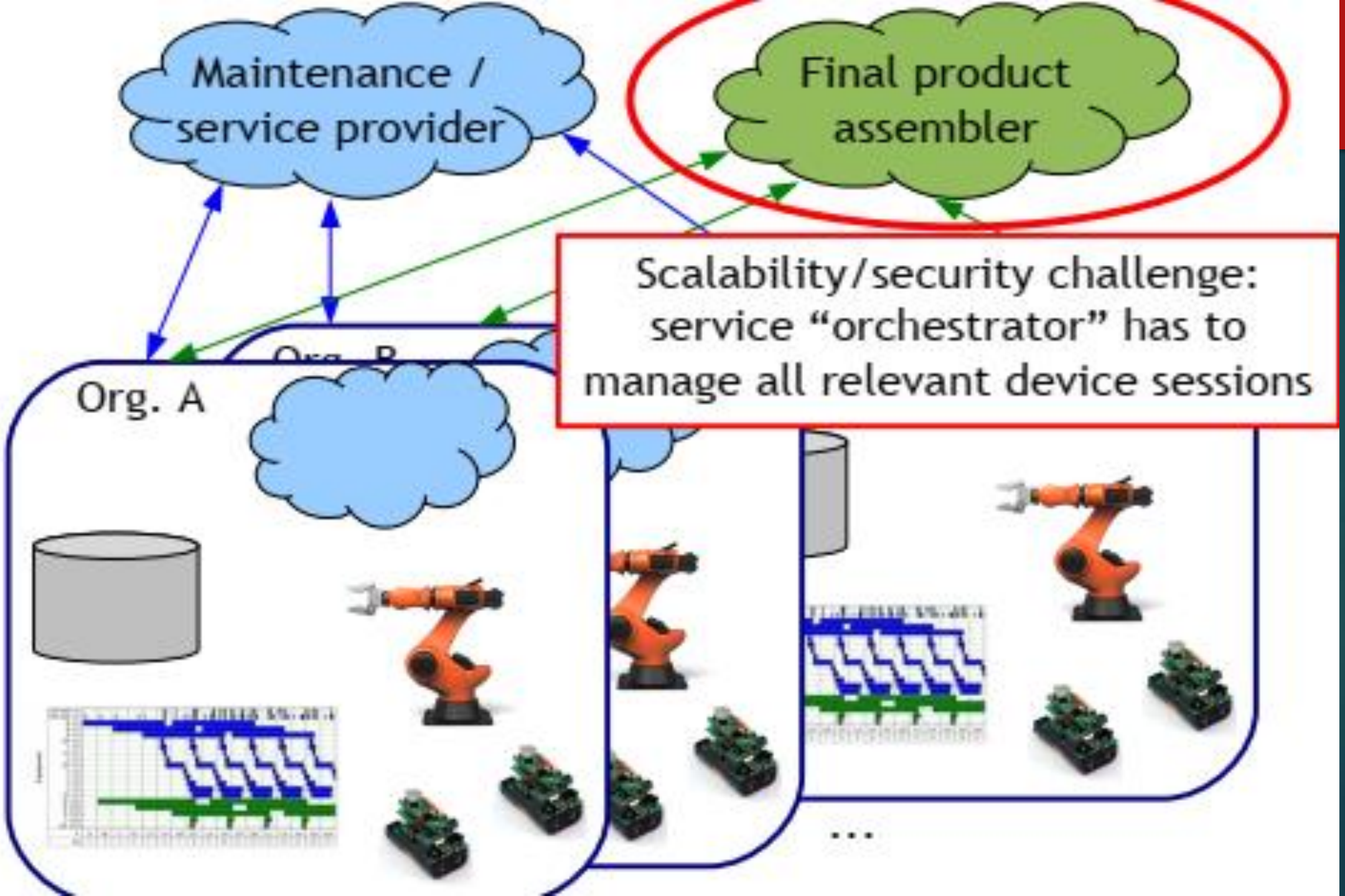
VÍ DỤ 1: IOT CÔNG NGHIỆP


Maintenance / service provider
Final product assembler
Org. A
Org. N

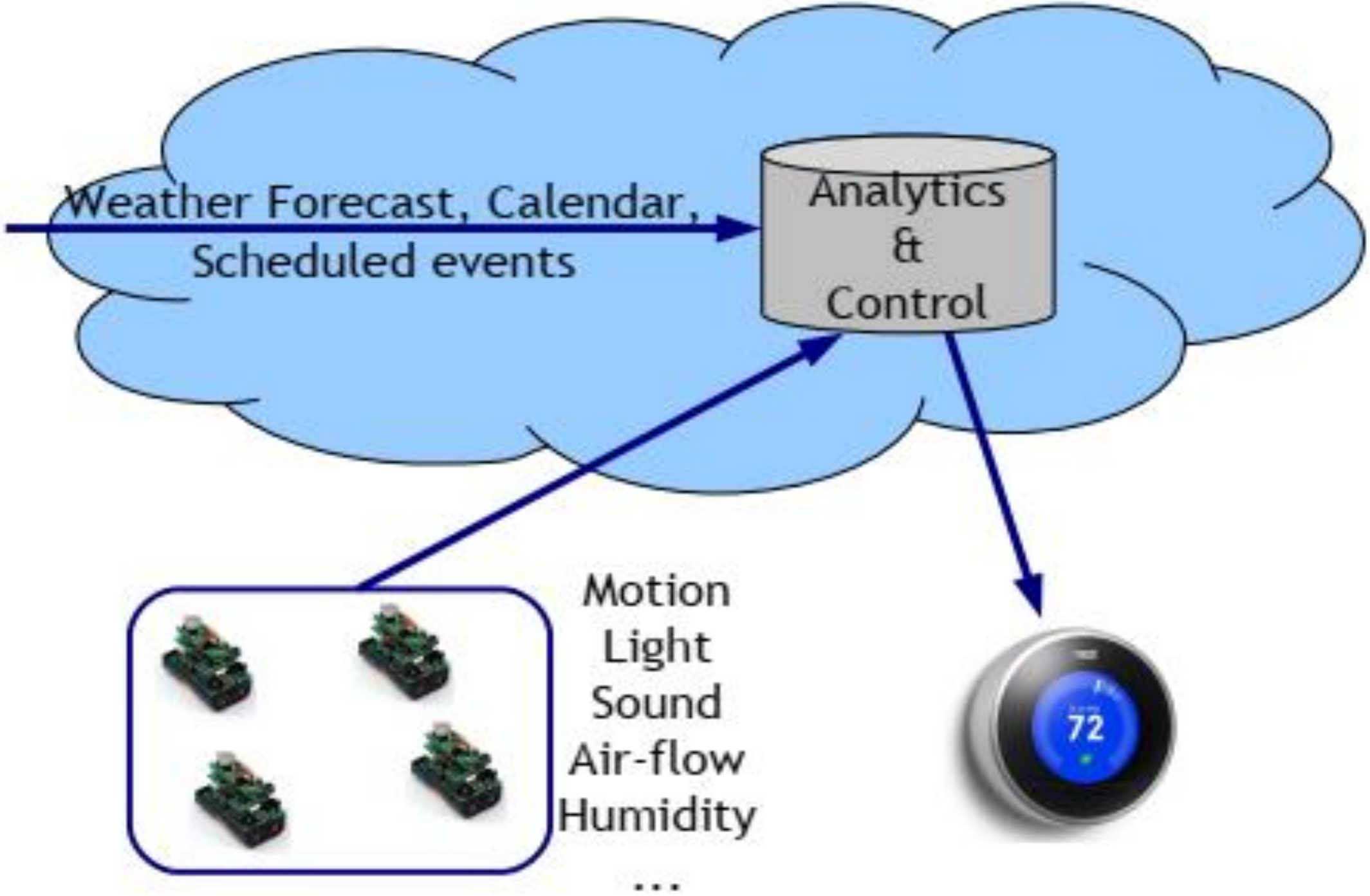

Maintenance / service provider
Final product assembler
Org. A
Org. N
...
ALERT: Broken robot arm!
...

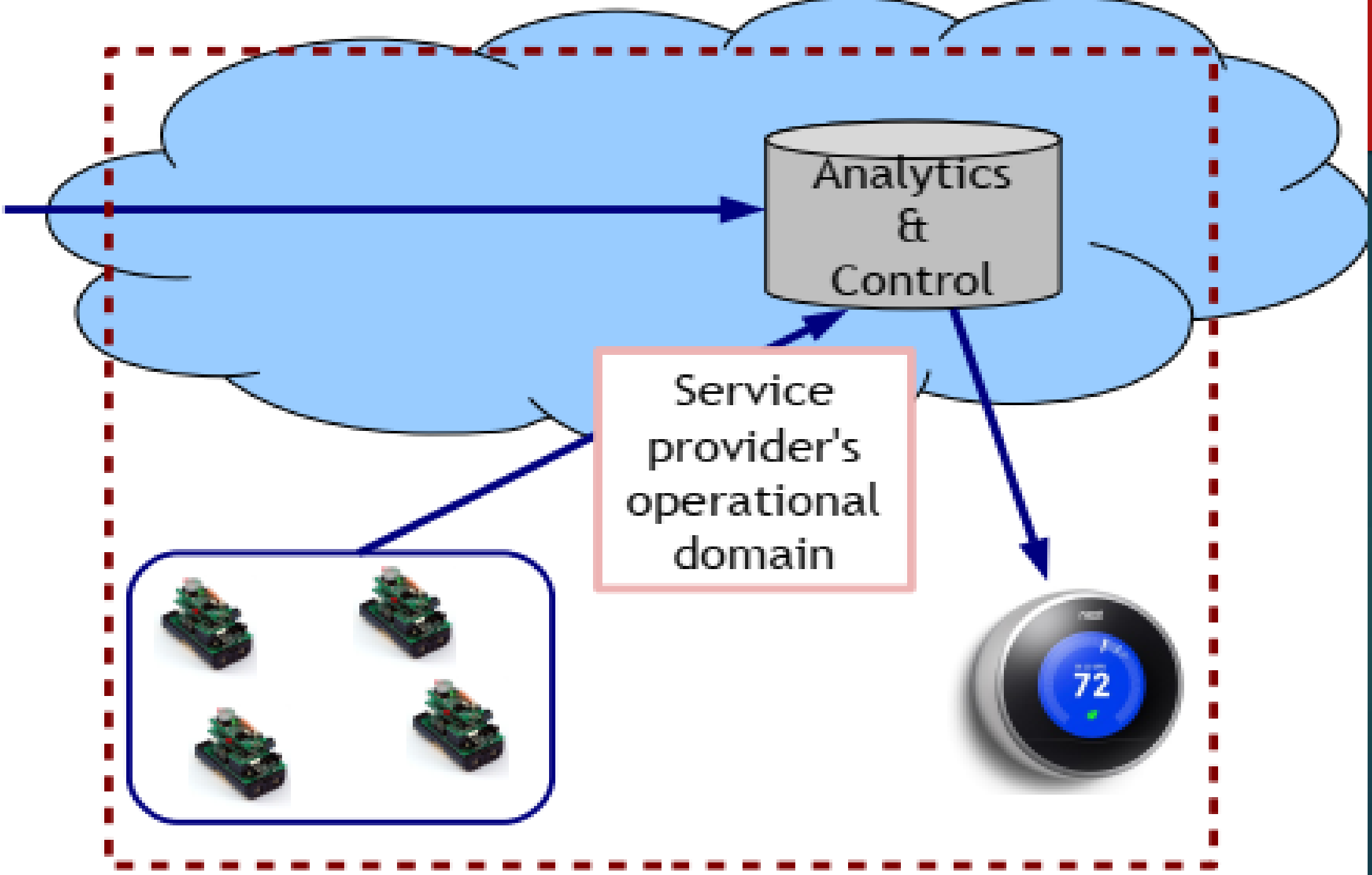

Maintenance / service provider
Final product assembler
...
Org. N
Org. A
ALERT: Broken robot
Security challenge: resource-limited device has to manage an external secure session

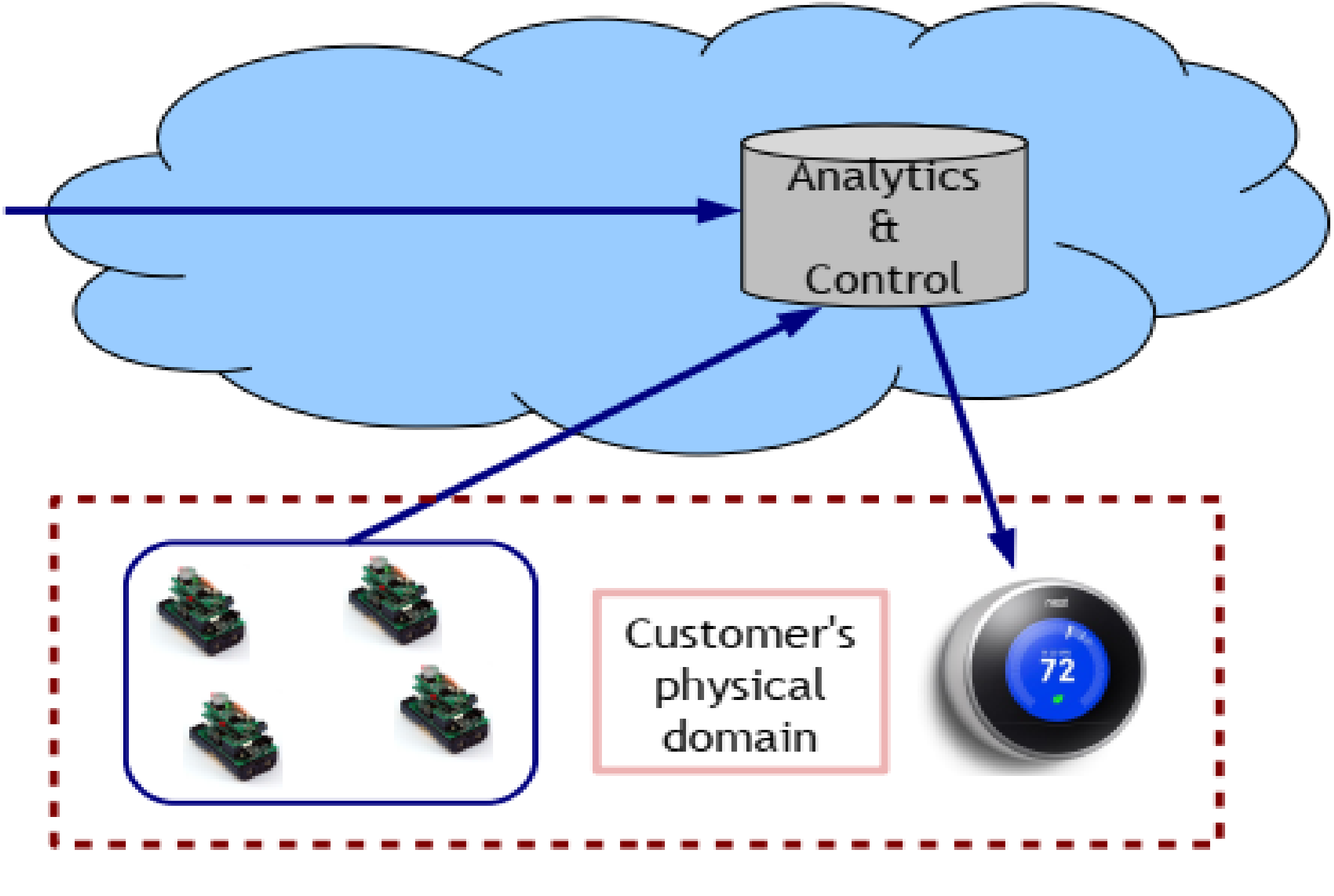

Maintenance / service provider
Final product assembler
...
Org. N
Org. A
ALERT: Broken robot arm!
Policy challenge: how to regulate which providers/orgs can access data?

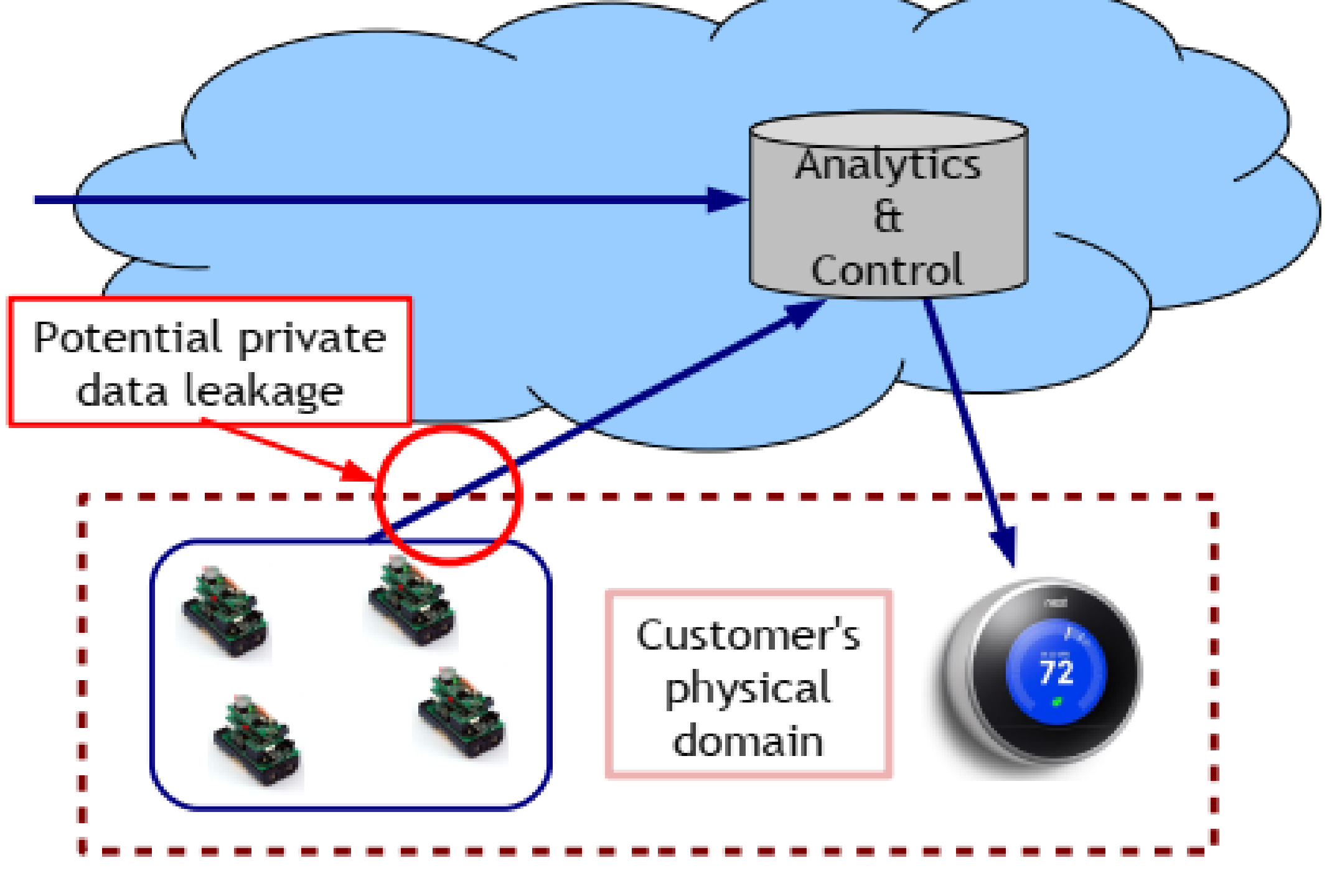

Maintenance / service provider
Final product assembler
Scalability/security challenge: service "orchestrator" has to manage all relevant device sessions
Org. A
...

VÍ DỤ 2: IOT ĐẤT Ở


Weather Forecast, Calendar,
Scheduled events
Analytics
&
Control
Motion
Light
Sound
Air-flow
Humidity
...
72

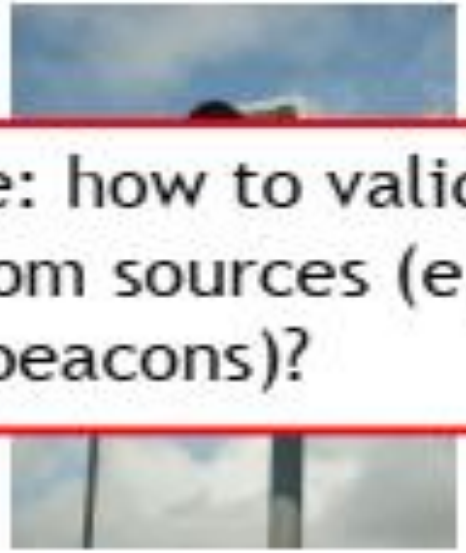

Analytics
&
Control
Service
provider's
operational
domain
72


Analytics
&
Control
Customer's
physical
domain
72


Analytics
&
Control
Potential private
data leakage
Customer's
physical
domain
72

VÍ DỤ 3: IOT ĐÔ THỊ/DÂN DỤNG

Security challenge: how do devices discover each other and ***verify*** who they discovered?



Security challenge: how to validate measurements from sources (e.g., sensors, beacons)?

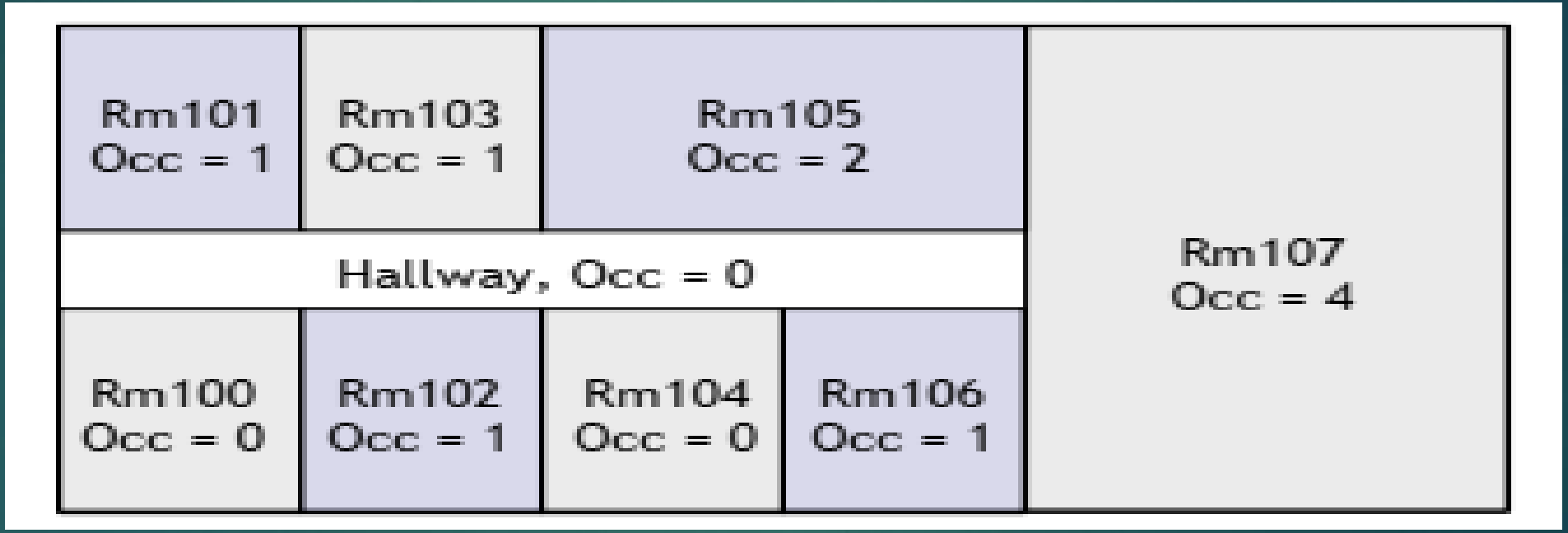
CÁC VẤN ĐỀ TẬP TRUNG DỮ LIỆU

- Ai sở hữu dữ liệu?
  - Ngoài ra, ai là người xác định ai sở hữu dữ liệu cảm biến?
- Làm cách nào để theo dõi nơi dữ liệu được tạo, vận chuyển, phân tích, lưu trữ, sử dụng làm đầu vào, v.v.?
- Dữ liệu nào là cần thiết?
  - Ứng dụng của bạn có cần dữ liệu cảm biến thô làm đầu vào hay thứ gì khác là đủ?
- Thông tin gì được chuyển tải trong dữ liệu?
  - Ứng dụng của bạn có thể học được gì từ dữ liệu của tôi?

KHI NÀO THÌ THÔNG TIN NHIỀU HƠN DỮ LIỆU?

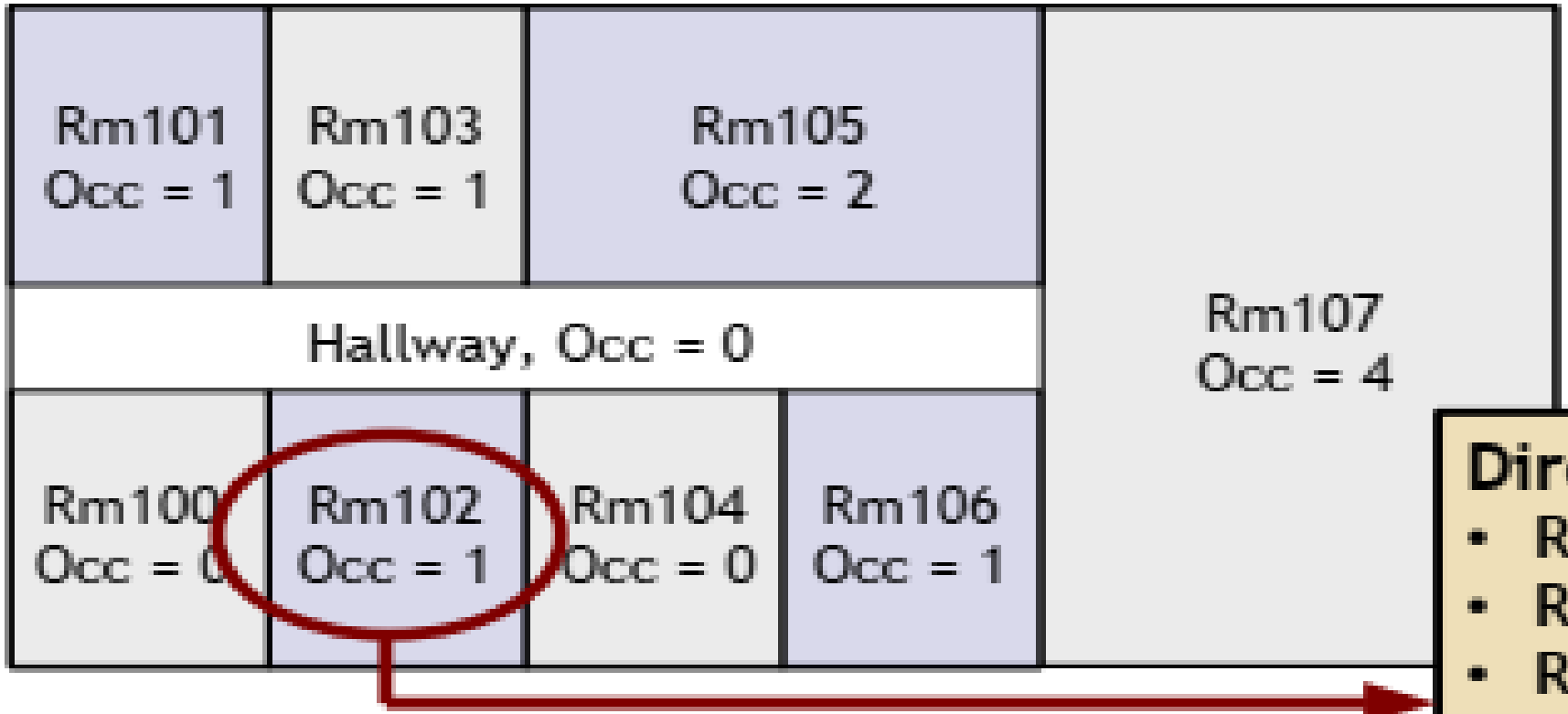
SỨC CHỨA

- Sức chứa = # người trong phòng
- Một tổ hợp cảm biến rất có giá trị cho hệ thống green HVAC



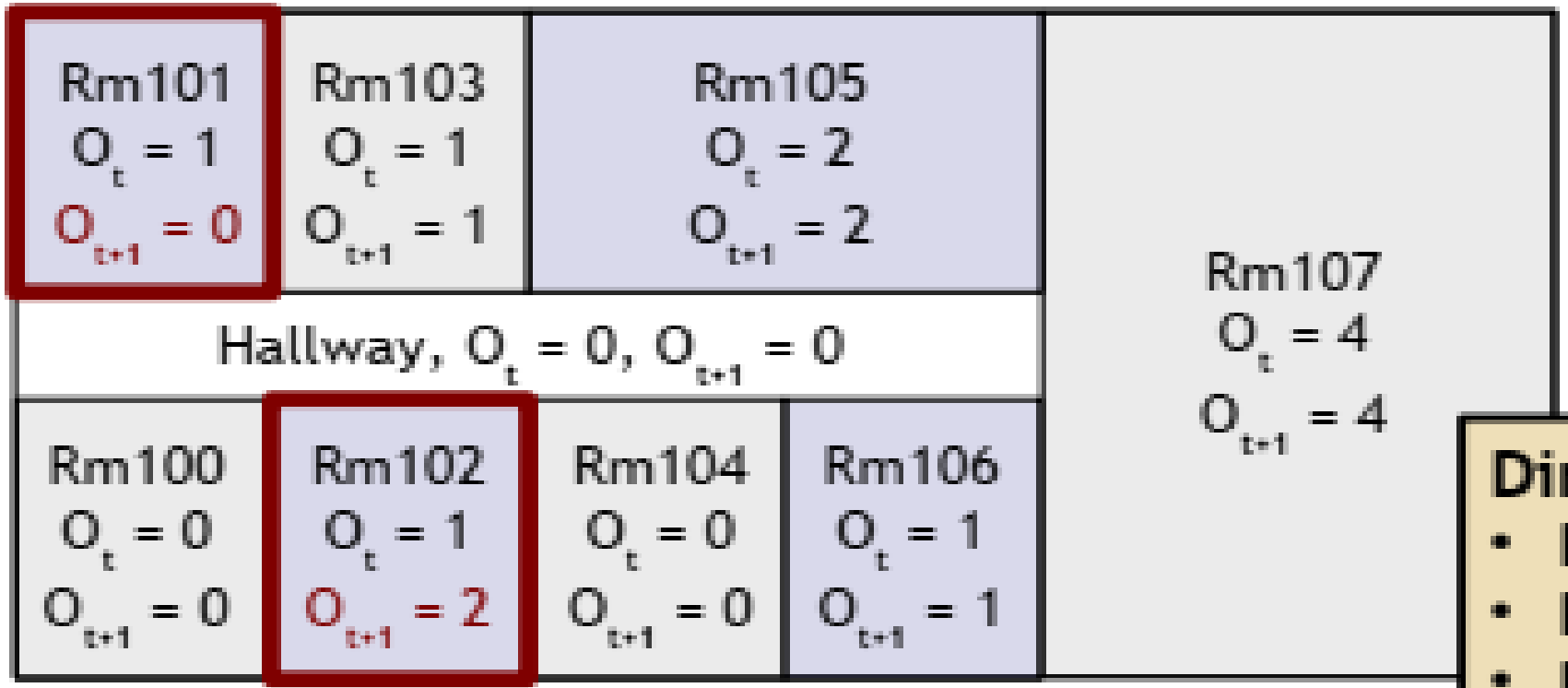
Thật hấp dẫn khi nói rằng chiếm chỗ là bảo vệ quyền riêng tư (trên thực tế, nhiều người đã nói như vậy)

SỨC CHỨA + BỐI CẢNH



Directory:

- Rm100: Aaron's office
- Rm101: Beth's office
- Rm102: Carlos's office
- Rm103: Dennis's office
- Rm104: Evelyn's office
- Rm105: Shared lab
- Rm106: Kitchen
- Rm107: Boardroom



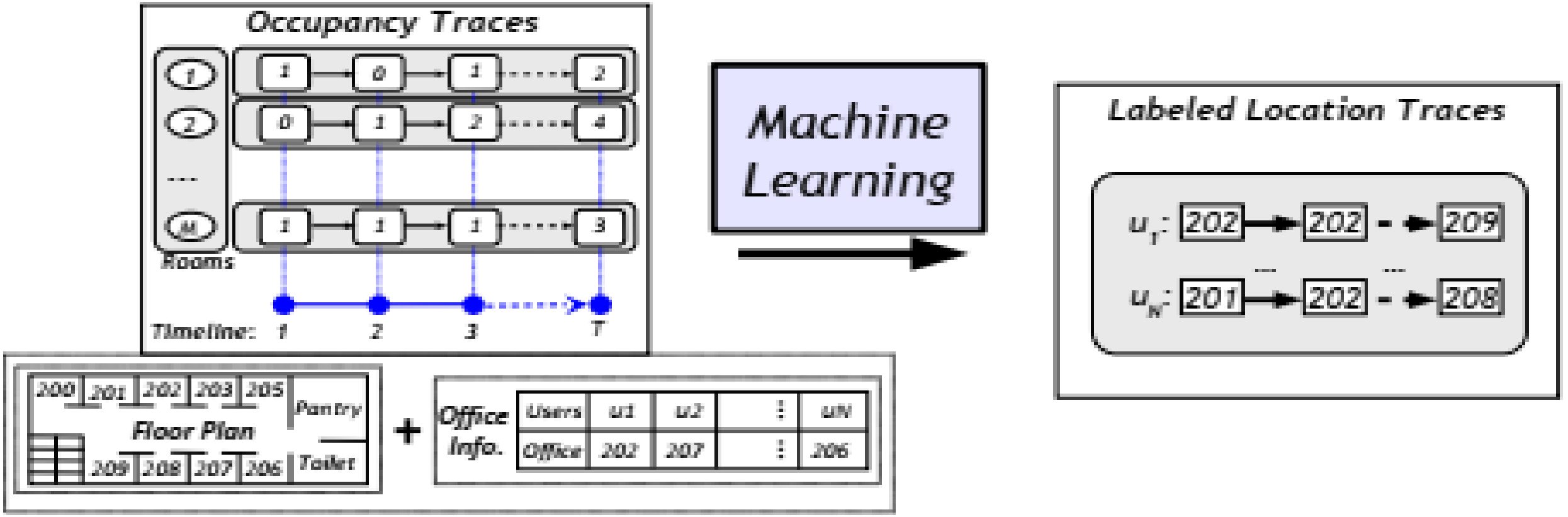
Directory:

- Rm100: Aaron's office
- Rm101: Beth's office
- Rm102: Carlos's office
- Rm103: Dennis's office
- Rm104: Evelyn's office
- Rm105: Shared lab
- Rm106: Kitchen
- Rm107: Boardroom

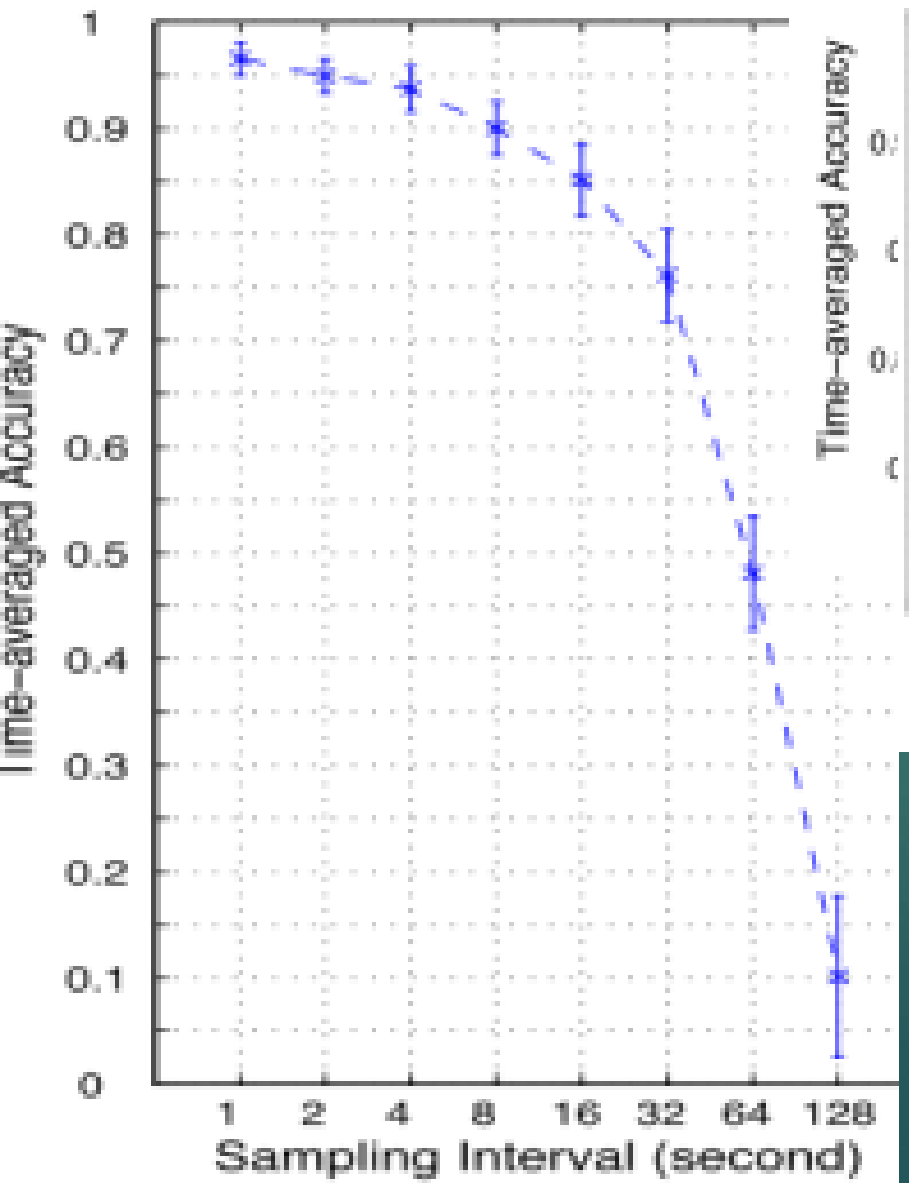
SỨC CHỨA – THEO DÕI

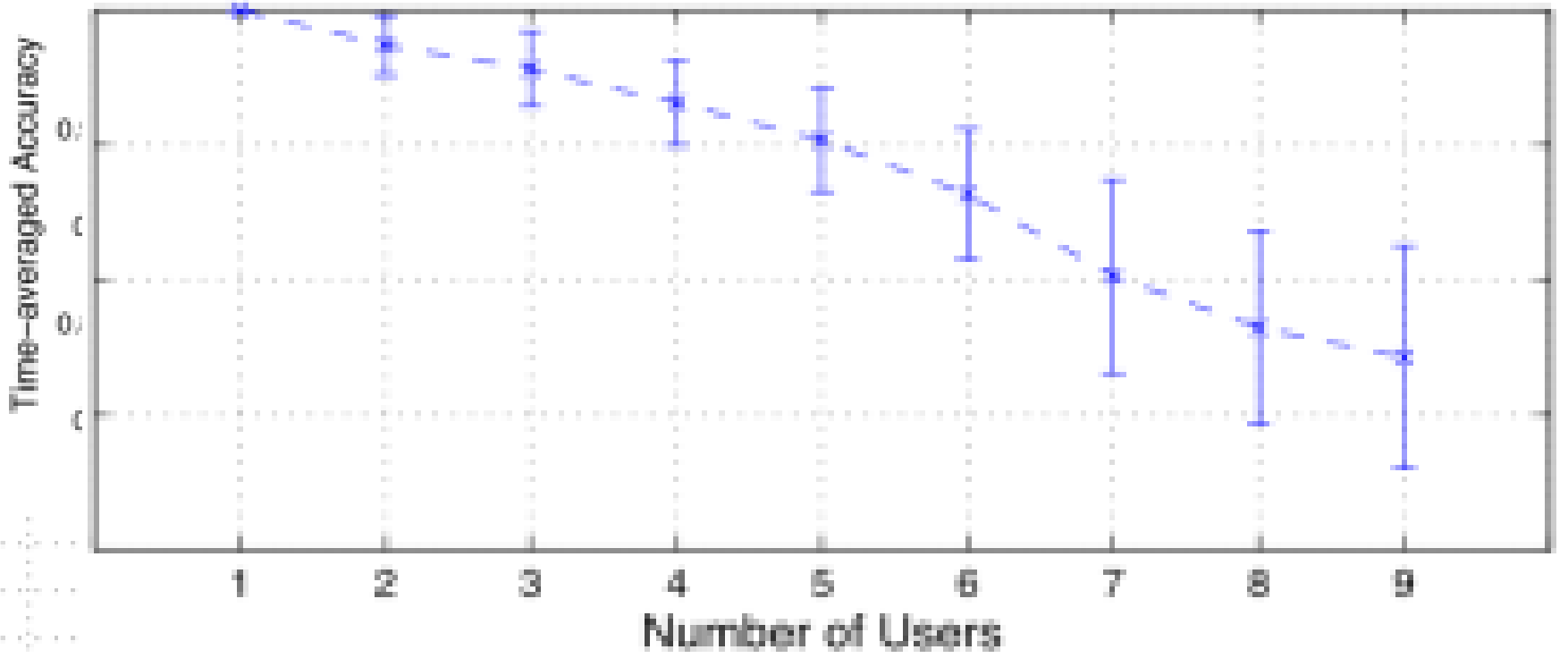
Dữ liệu chiếm đầy đủ chi tiết cho phép tái tạo lại dấu vết vị trí của người dùng tòa nhà

Thông tin ngữ cảnh cho phép gắn nhãn dấu vết vị trí với danh tính người dùng



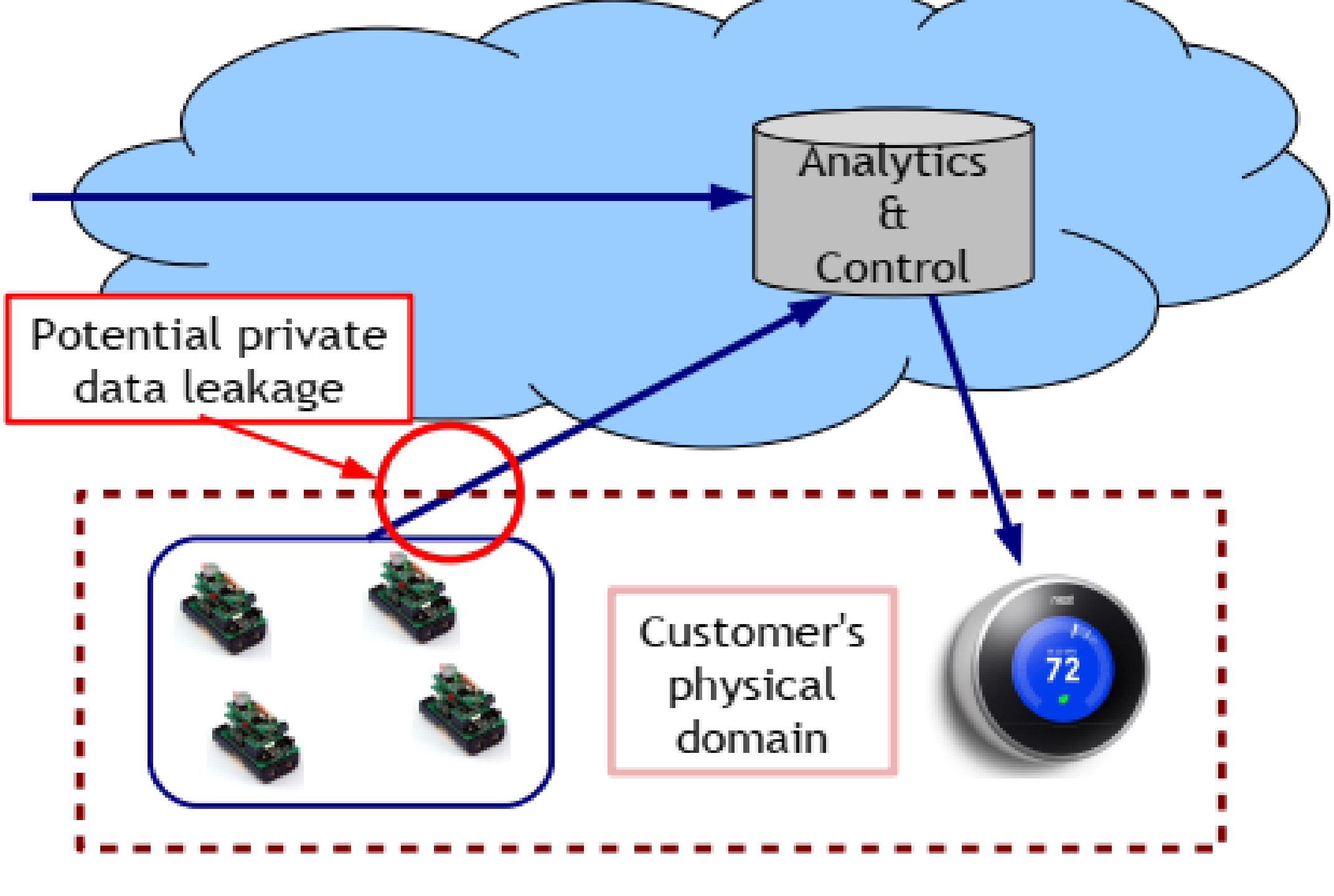
ĐỘ CHÍNH XÁC -> RỦI RO VỀ QUYỀN RIÊNG TƯ

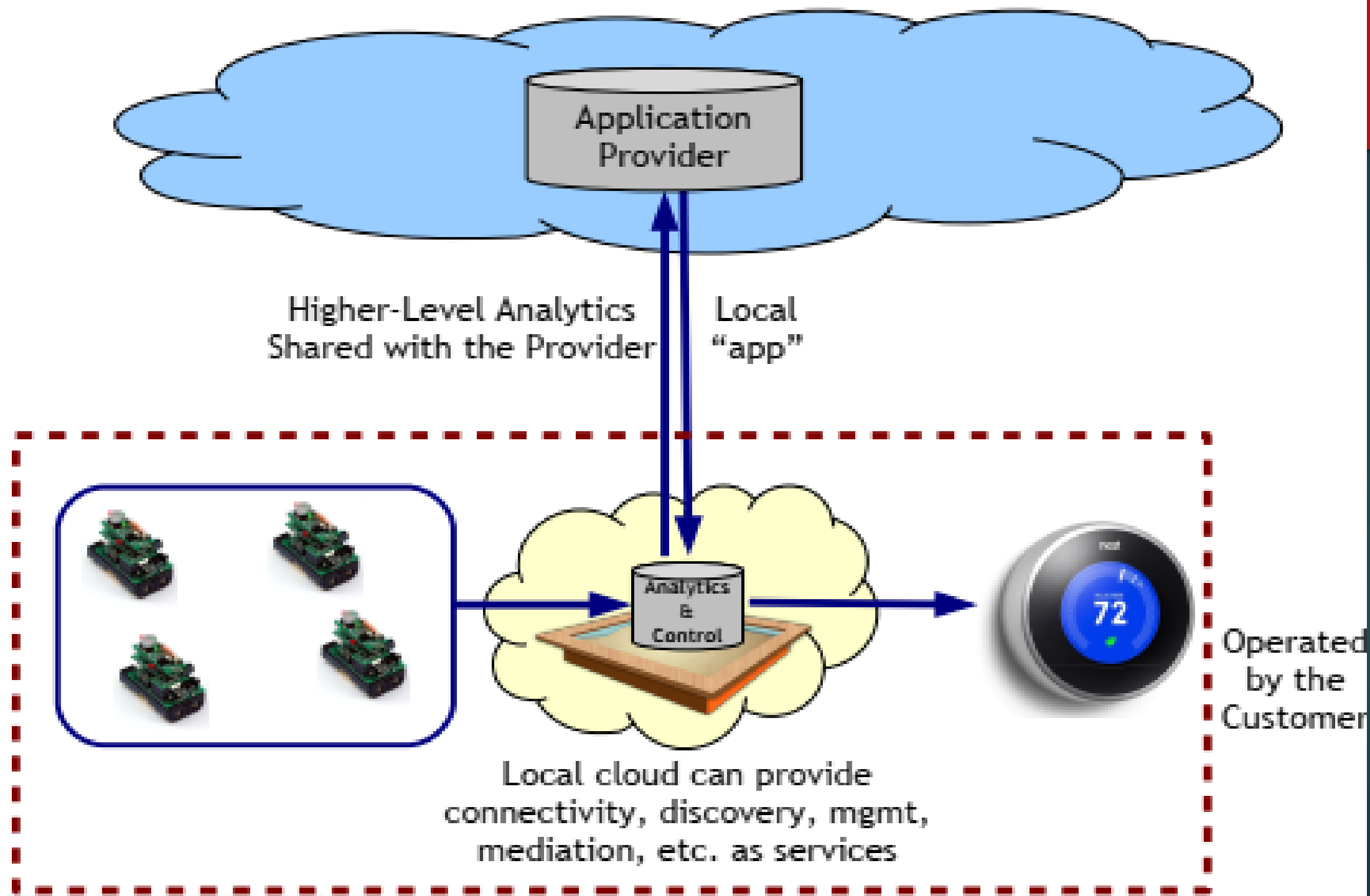




Bộ dữ liệu điểm chuẩn Augsburg với dữ liệu tổng hợp; Ước tính bằng thuật toán FHMM + Viterbi đã sửa đổi

LÀM THẾ NÀO CHÚNG TA CÓ THỂ GIẢI QUYẾT NHỮNG VẤN ĐỀ NÀY?

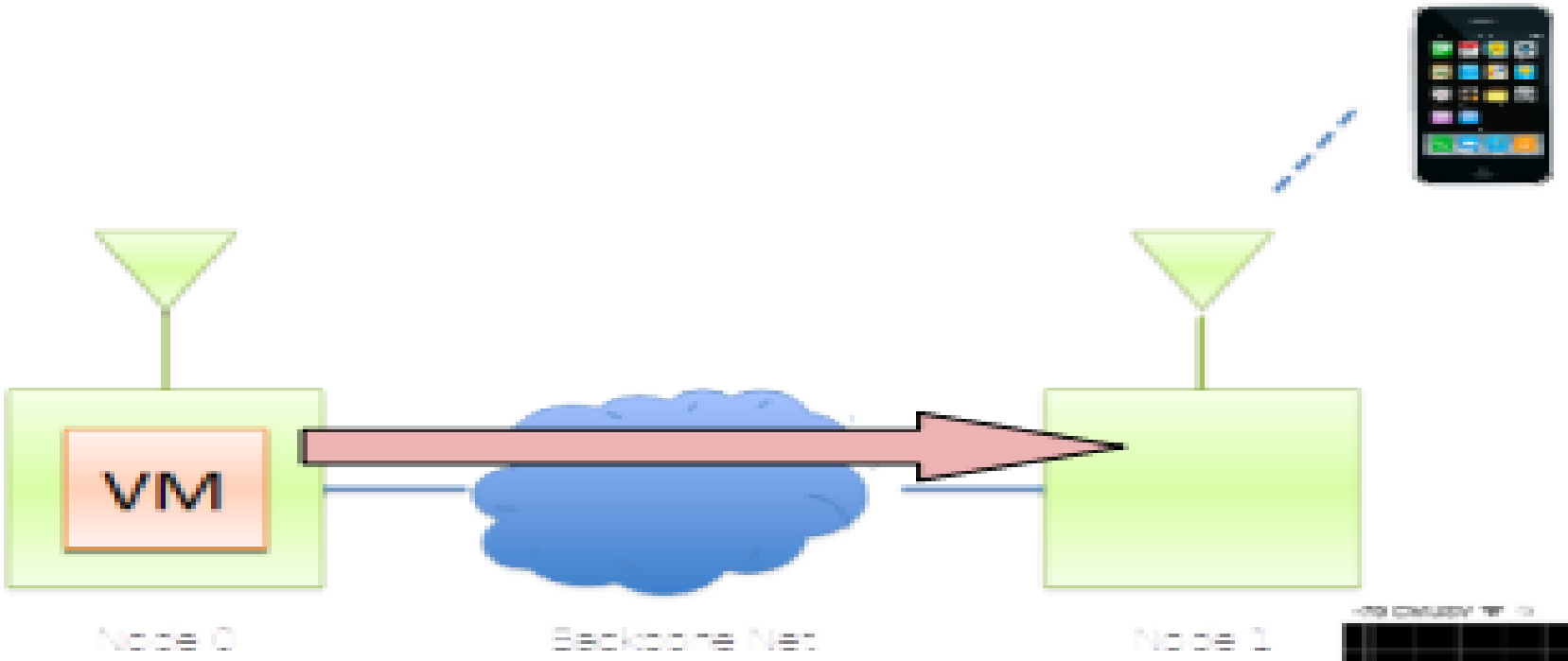

Analytics
&
Control
Potential private
data leakage
Customer's
physical
domain
72

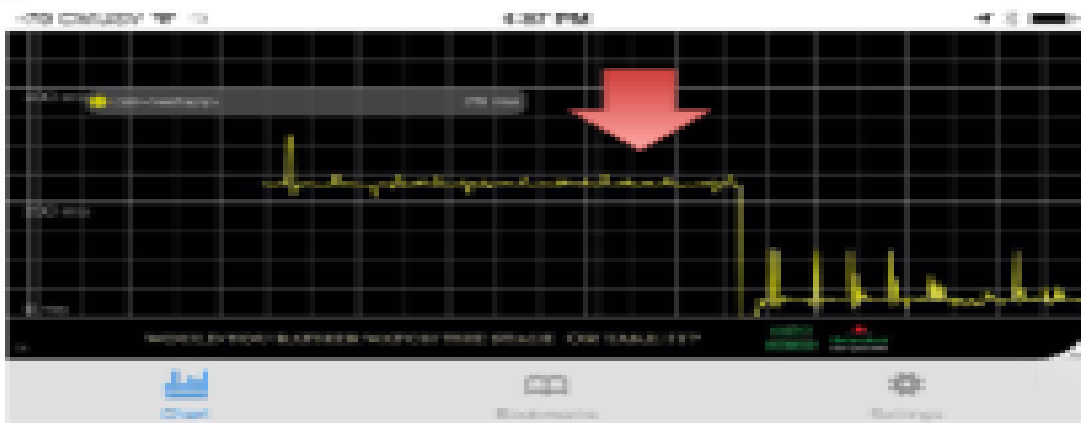

Application Provider
Higher-Level Analytics Shared with the Provider
Local "app"
Analytics & Control
72
Operated by the Customer
Local cloud can provide connectivity, discovery, mgmt, mediation, etc. as services

MỘT VÀI CÂN NHẮC

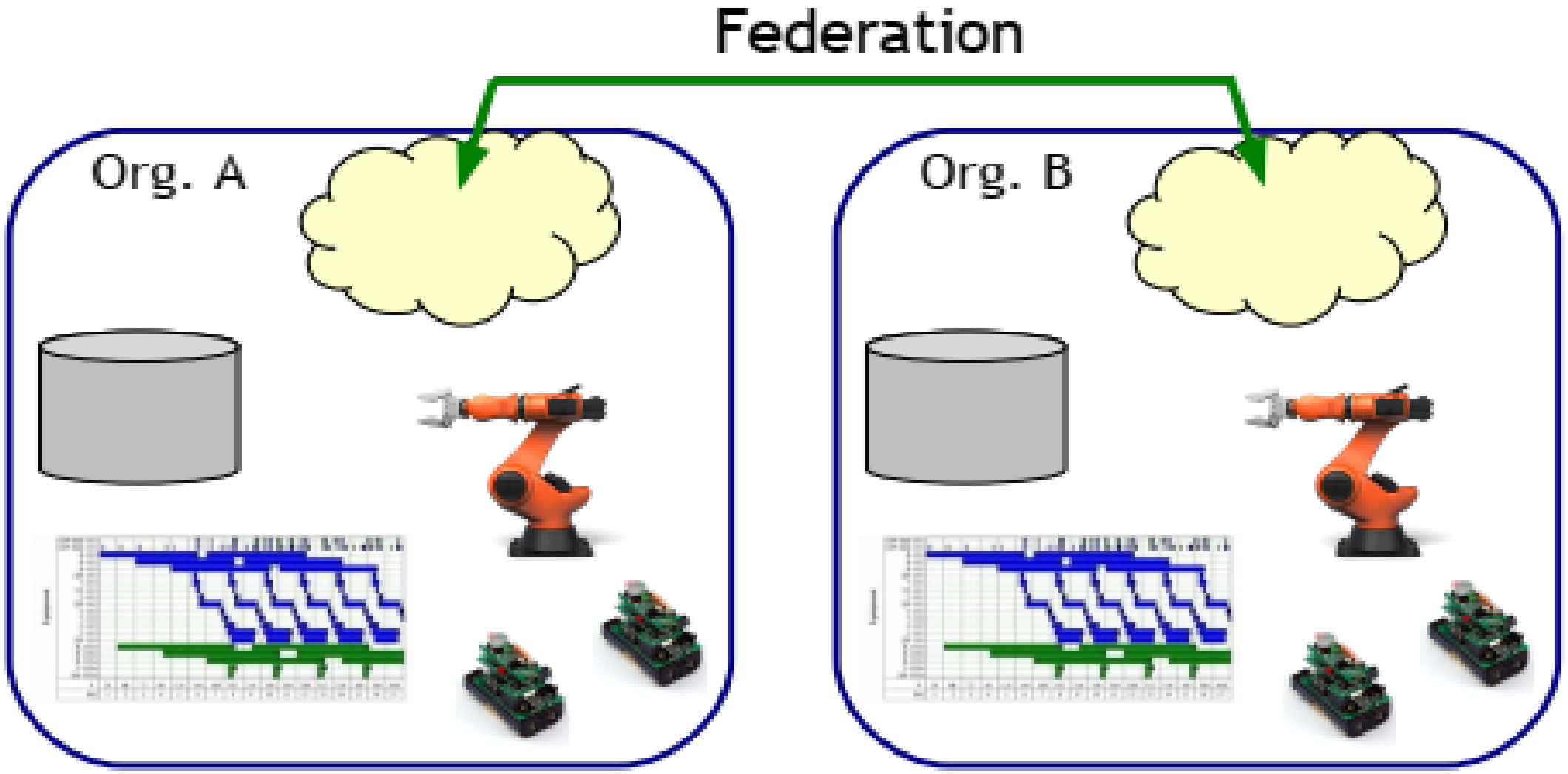
- Tài nguyên đám mây cục bộ có thể sử dụng các nguyên tắc điện toán đáng tin cậy để lưu trữ an toàn phần mềm của bên thứ 3 (giống như điện thoại di động)
- Cổng trung gian có thể chủ động kiểm soát luồng thông tin giữa các thiết bị nội bộ và tài nguyên của bên thứ ba
- Di chuyển tích cực trong miền cục bộ có thể giúp đáp ứng (gần) các yêu cầu CPS thời gian thực

Migration

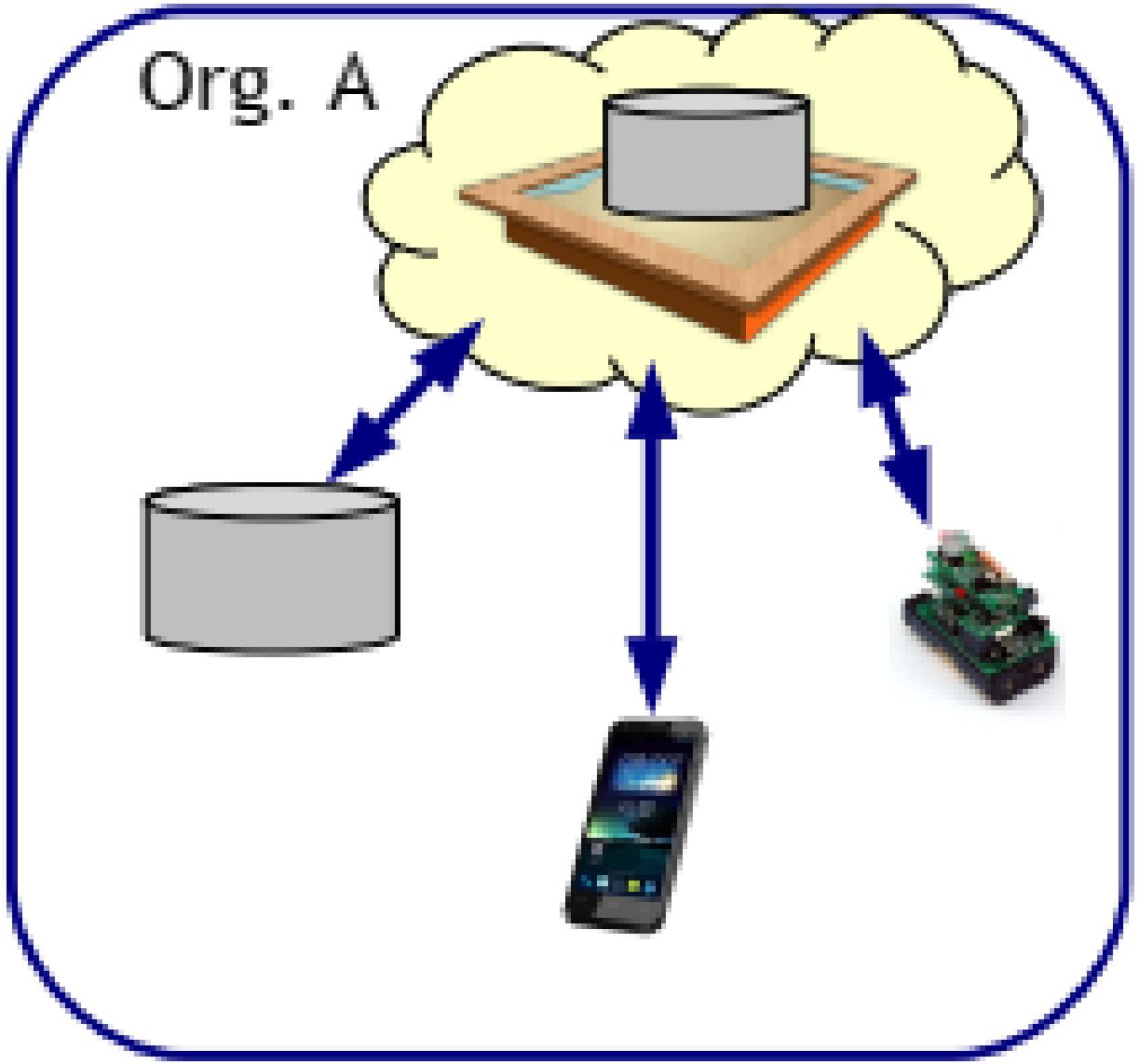




How could two orgs collaborate in a constructive, efficient, privacy-preserving, … manner?



MÔ HÌNH MIỀN IOT TỔNG QUÁT



Nội bộ miền: mọi thứ được quản lý cục bộ/riêng tư bởi bộ điều khiển miền

Liên miền: bộ điều khiển miền khởi tạo, dàn xếp và quản lý các tương tác

ĐIỂM MANG ĐI - TAKE-AWAY POINTS

- IoT # Internet (hoặc WoT # Web)
- Mô hình liên kết/hòa giải miền cho phép kiểm soát chi tiết hơn hoạt động cộng tác, chia sẻ, v.v. phổ biến đối với các ứng dụng IoT
- Mô hình miền có những thách thức riêng nên còn rất nhiều việc phải làm

BÀI 21:

BẢO MẬT & QUYỀN RIÊNG TƯ CỦA MẠNG VIỄN THÔNG