IoT Week, 6-9 June 2017

There is No Perimeter in IoT Security

Andrei Robachevsky
robachevsky@isoc.org

Despite the global buzz around the Internet of Things, there is no single, universally accepted definition for the term…

A **trend** where a large number of embedded devices employ communication services offered by the Internet protocols (IAB)

A global **infrastructure** […] interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies (ITU-T)

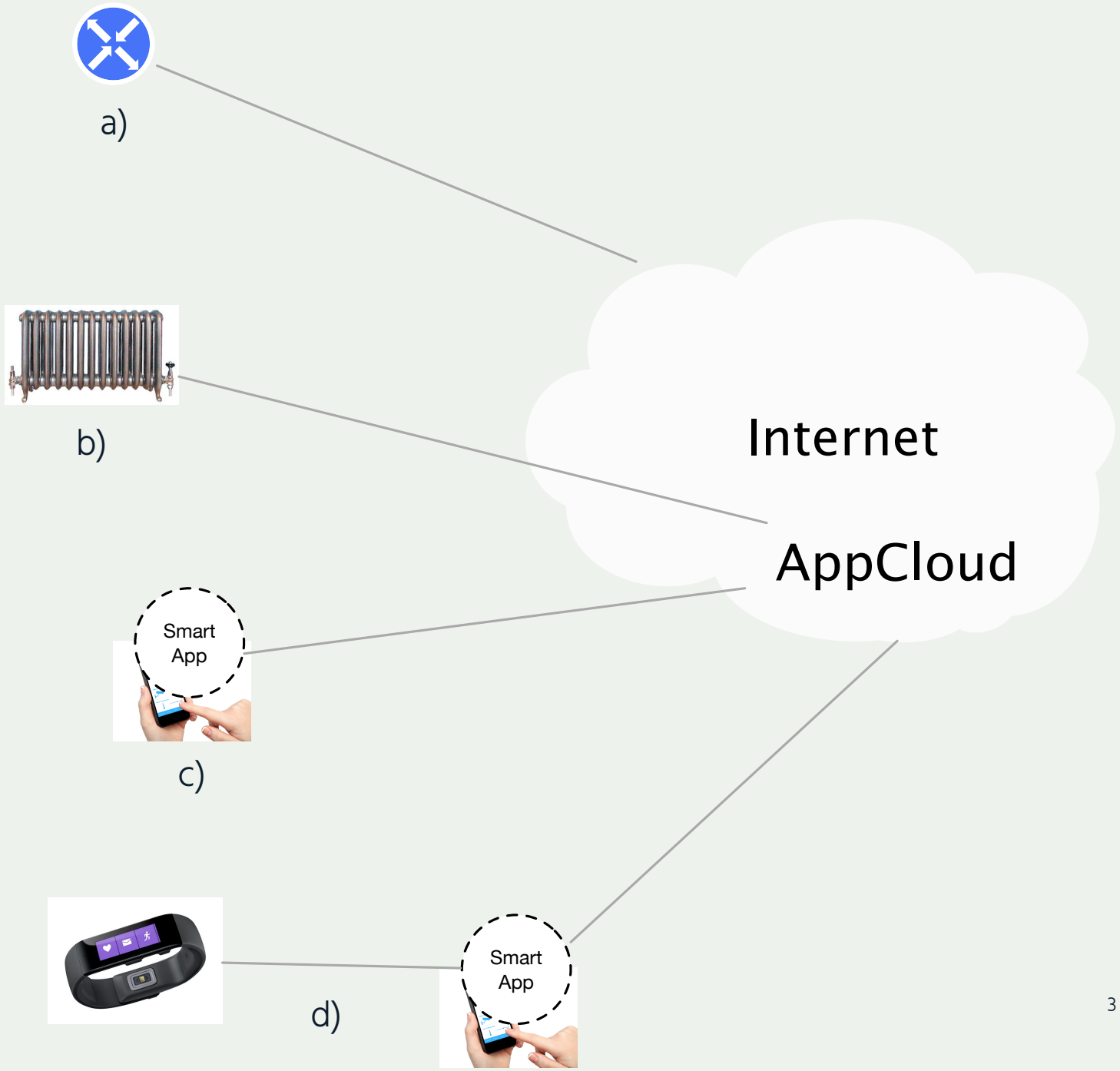
From a broader perspective, the IoT can be perceived as a **vision** with technological and societal implications (ITU-T)

The Internet of Things (IoT) is a **framework** in which all things have a representation and a presence in the Internet (IEEE)

The **extension** of network connectivity and computing capability to objects, devices, sensors, and items not ordinarily considered to be computers (ISOC)

Which configuration better describes the IoT?

1. a)
2. b)
3. b), c), d)
4. All of the above
5. None of the above

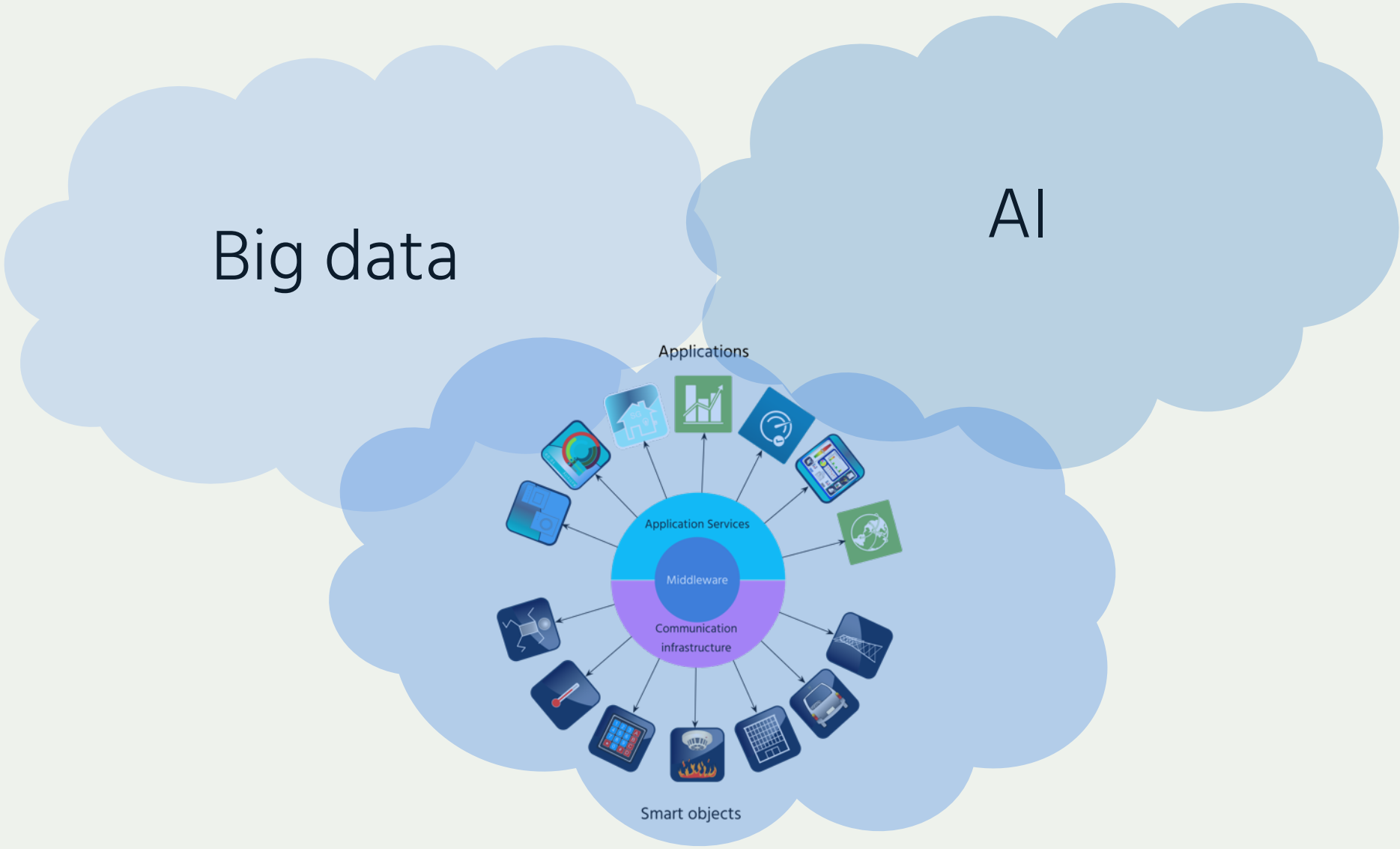


IoT is a system

The Internet of Things (IoT) is not just a device connected to the Internet - it is a complex, rapidly evolving system.

To understand the implications, analyse risks, and come up with effective security solutions we need to look ahead and take into account other components, such as Big Data and Artificial Intelligence (AI).

IoT is a system



Who is responsible?

To scale up we need a collective approach, addressing security challenges on all fronts.

The Online Trust Alliance IoT Security Framework provides a great foundation listing the baseline requirements for security and privacy.

Different threat scenarios – Different existing approaches and communities

IoT as a botnet

— DDoS attacks
— SPAM
— Other typical botnet activities

IoT as a privacy intruder (AI+BigData)

— Surveillance
— Espionage
— Data breaches

IoT as a security threat

— Misbehaving things/actuators, re-purposing
— Physical security
— Espionage/APT

How to ignite action?

Engaging Forces for Security

- Market forces
  - Recognising value of security
  - Affordable security

- Regulation forces
  - Compliance: product and the ISM processes
  - Facilitator rather than enforcer

- Societal forces
  - All parties involved are interested in innovative and security IoT
  - Norm setting
  - Finding points of maximum impact

Is paradigm shift needed?

Yes

- Scale and speed of deployment
- Security means Safety
- Issues are amplified by BigData and AI