What could possibly go wrong

IoT meets The Law

Key for IoTDI, Berlin
4 April 2016

Jon Crowcroft
jon.crowcroft@cl.cam.ac.uk

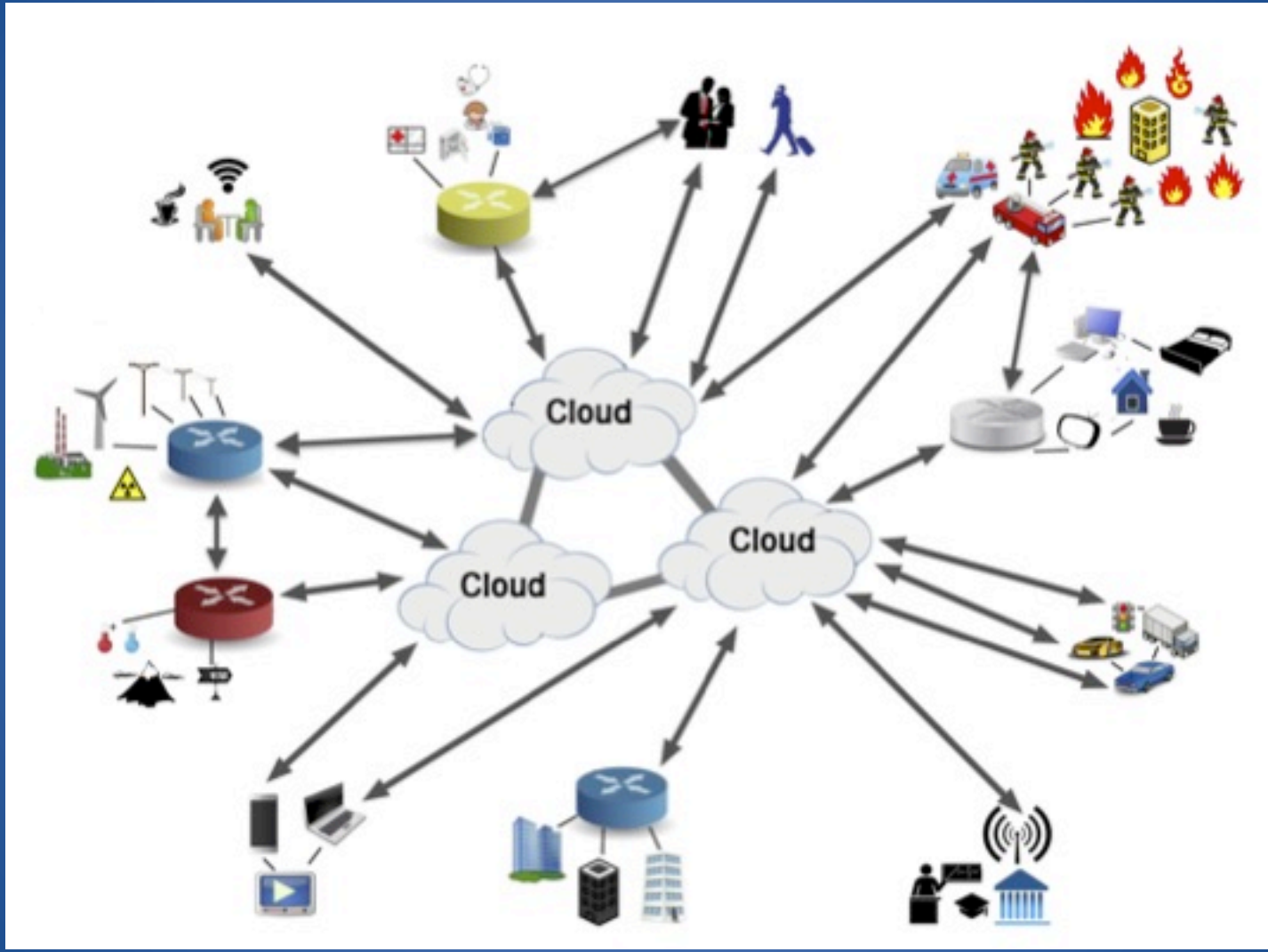
Christopher Millard
c.millard@qmul.ac.uk

Ian Walden
i.n.walden@qmul.ac.uk

UNIVERSITY OF CAMBRIDGE

Queen Mary University of London

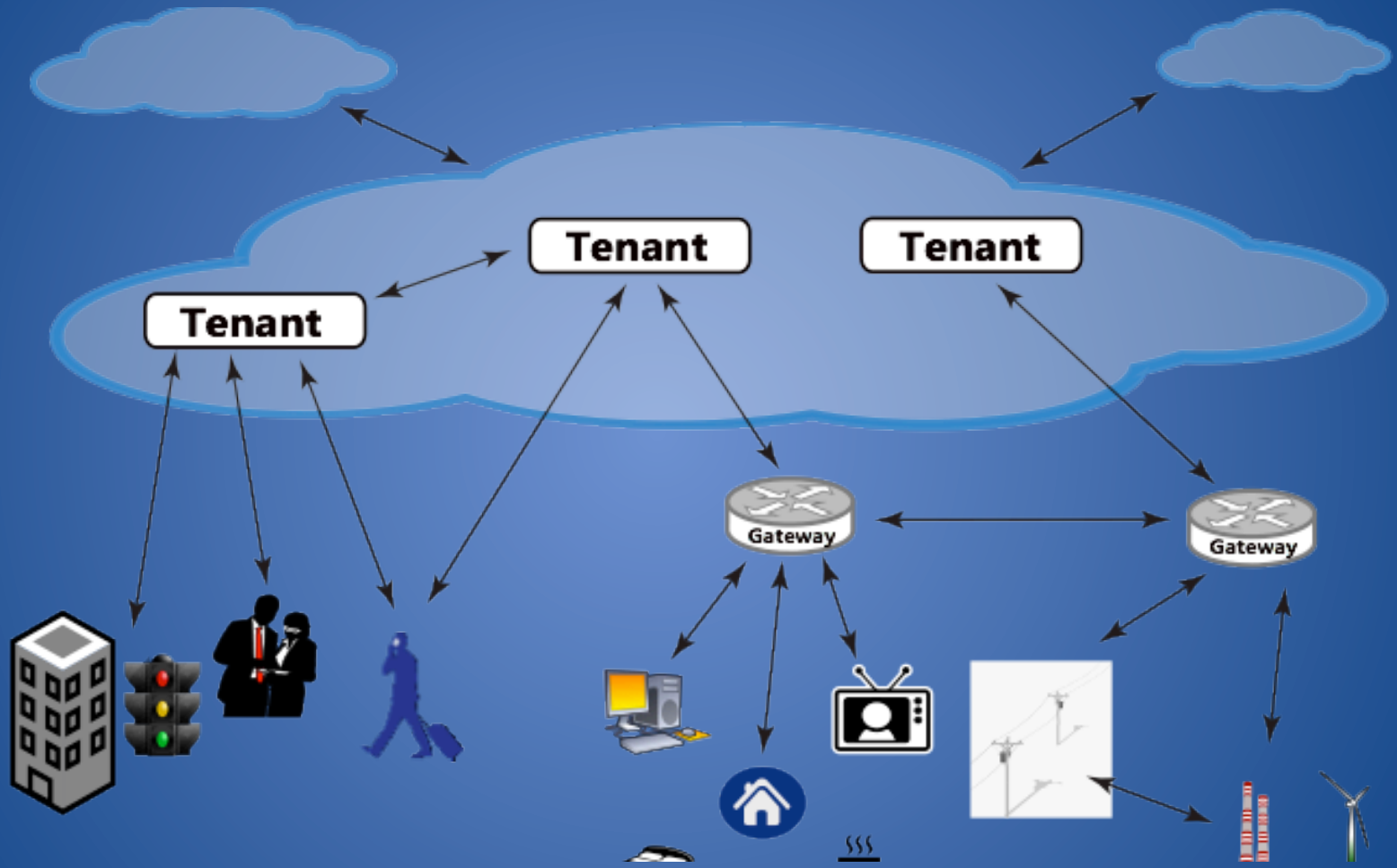
IoT Technical Considerations – Big Picture



UNIVERSITY OF CAMBRIDGE

Queen Mary University of London

Interactions twixt IoT & Cloud



UNIVERSITY OF CAMBRIDGE

Queen Mary University of London

Clouds of Things: Technical Considerations (Confidentiality, Integrity, Availability)

1. Secure communications (C, I): Work is advanced and existing techniques can be leveraged. IoT could benefit from lighter-weight schemes, particularly where cryptography is involved.
2. Access controls for IoT-Cloud (C): Standard mechanisms can be used. IoT adds complexity due to the scale and dynamism of 'thing' access.
3. Identifying sensitive data (C): Largely a non-technical concern, but has an impact on how policies are defined.
4. Public, private or hybrid? (C, A): Currently blunt partitioning is supported, but emerging research will allow for more flexible deployments that facilitate data sharing.
5. In-cloud data protection (C): There are strong isolation techniques available and providers employ general access controls. More flexible approaches are needed for inter-application sharing to be possible (see 6, below).
6. In-cloud data sharing (C, A): Inter-application sharing is needed for IoT but currently is not part of the cloud philosophy.
7. Encryption by 'things' (C, I): Encryption techniques are mature, but this approach precludes most computations on protected data and involves complex key management. Ongoing work into homomorphic encryption will assist. Lightweight encryption mechanisms are being developed and will require robust testing and analysis.

Clouds of Things: Technical Considerations (Confidentiality, Integrity, Availability)

8. Data combination (C): Some techniques exist to prevent user re-identification, but much more work is needed.
9. Identifying ‘things’ (C): Existing work on identity management can be leveraged for IoT, but more experience at a larger scale is needed to determine suitability and/or limitations.
10. Identifying the provider (C): The basic issues are mostly architectural or configuration concerns. Some outstanding issues remain when resources are shared or where decisions need to be made at runtime.
11. Increase in interactions and data load (A): Cloud services manage elasticity well, but resource expansion is not unlimited. Peak IoT loads are unknown, but possibly controlled by economics (payment/ownership).
12. Logging at large scale (C, I, A): Currently logging is low-level and system-centered. More work is needed on logging and processing tools for applications and users.
13. Malicious ‘things’—protection of provider (C, I, A): Existing techniques can be deployed.
14. Malicious ‘things’—protection of others (C, I, A): There are potentially techniques that can assist. Experience is needed of cloud services operating across IoT subsystems.

Clouds of Things: Technical Considerations (Confidentiality, Integrity, Availability)

15. Certification of cloud service providers (C, I, A): This is currently manual and static, leading to delays when updates are required. Research is needed on automatic certification processes, possibly including hardware-based solutions.
16. Trustworthiness of cloud services (C, I, A): An emerging field with ongoing research. Experience of practical implementation is needed.
17. Demonstrating compliance using audit (C, I, A): Currently, the compliance of cloud providers to their contractual obligations is not demonstrated convincingly. Research is needed, and IoT will add additional complexity.
18. Responsibility for composite services (C, I, A): The legal implications of the use of third-party and other services are unresolved. Such usage is not as yet transparent to tenants and/clients. More work is needed concerning user and application-level policy aspects.
19. Compliance with data location regulations (C, I, A): Currently not enforceable except at coarse granularity. There is research in IFC that can assist, but the concepts are not yet commercially deployed.
20. Impact of cloud decentralisation (C, I, A): This is an emerging field, where the current focus is on functionality. More attention is needed regarding security.

Clouds of Things: Relationships + Responsibilities

- Relevant parties, their roles, and the contract ecosystem
- Establishing contractual relationships using things
- Who owns what?
- Potential non-contractual sources of liability
- Cyber-risk and insurance
- Developing a taxonomy for the purposes of legal analysis

UNIVERSITY OF CAMBRIDGE

Queen Mary University of London

Personal Data in Clouds of Things

- What is regulated as personal data?
- Who is responsible?
- Which laws apply?
- What rights to individuals have?
- How do rules on data location and data transfer work?

UNIVERSITY OF CAMBRIDGE

Queen Mary University of London

Governance of Clouds of Things

- Surveillance issues
- Identity and authentication
- Standards
- Demonstrating compliance with legal obligations
- Consumer protection
- Market and competition issues
- Use of radio spectrum

UNIVERSITY OF CAMBRIDGE

Queen Mary University of London

Clouds of Things: ‘Looking into the Nest’

- Contracting and Regulating for IoT
  - Case study
    - Not survey
  - Supply chain
    - Transparency
  - Actors & ecosystem
    - Owners, tenants, users

UNIVERSITY OF CAMBRIDGE

Queen Mary University of London

Clouds of Things: Layered ‘legals’

- Terms of Service (sites, web apps, mobile apps)
- EULA (embedded software)
- Sales terms (hardware)
- Privacy statement (for the devices)
- Website privacy policy (for monitoring data & accessing accounts)
- Open-source compliance
- IP and related notices
- Community Forum Agreement (user sharing)
- EU Declarations (type approval)
- Installation ToS
- Developer ToS

UNIVERSITY OF CAMBRIDGE

Queen Mary University of London

Clouds of Things: Private ordering & public control

- ‘Product’ as an inseparable mix of hardware and software and services and….
  - Liability standard: *Boston Scientific Medizintechnik GmbH v AOK Sachsen-Anhalt* (2015)
  - The ‘disconnected’ Thing?
- Modifications, interoperability & portability
  - User interactions
- Security & sharing
  - ‘the products will share information with each other’

UNIVERSITY OF CAMBRIDGE

Queen Mary University of London