Internet of Things and Smart Cities Security: Challenges and Issues

RAJ JAIN

Washington University in Saint Louis
Saint Louis, MO 63130
Jain@wustl.edu

Keynote at 1st Annual Research Workshop on Advances & Innovations in Cyber Security, Memphis, TN, June 10, 2016

These slides are available on-line at:
http://www.cse.wustl.edu/~jain/talks/iots_tns.htm

Overview

1. A Layered Model of IoT and Smart Cities
2. Challenges: Non-Technical and Technical
3. IoT/Smart City Security
4. Software Defined Secure Multi-Cloud Application Management for IoT

Trend: Smart Everything

Smart Watch

Smart TV

Smart Car

Smart Health

Smart Home

Smart Kegs

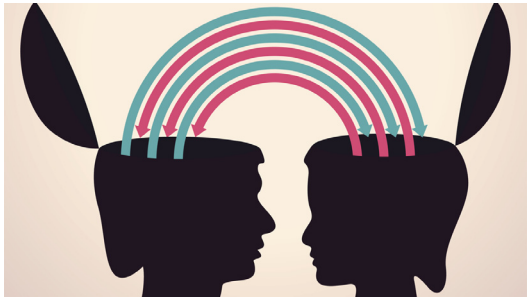
Smart Space

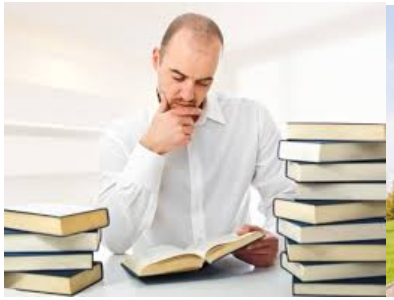
Smart Industries

Smart Cities

What's Smart?

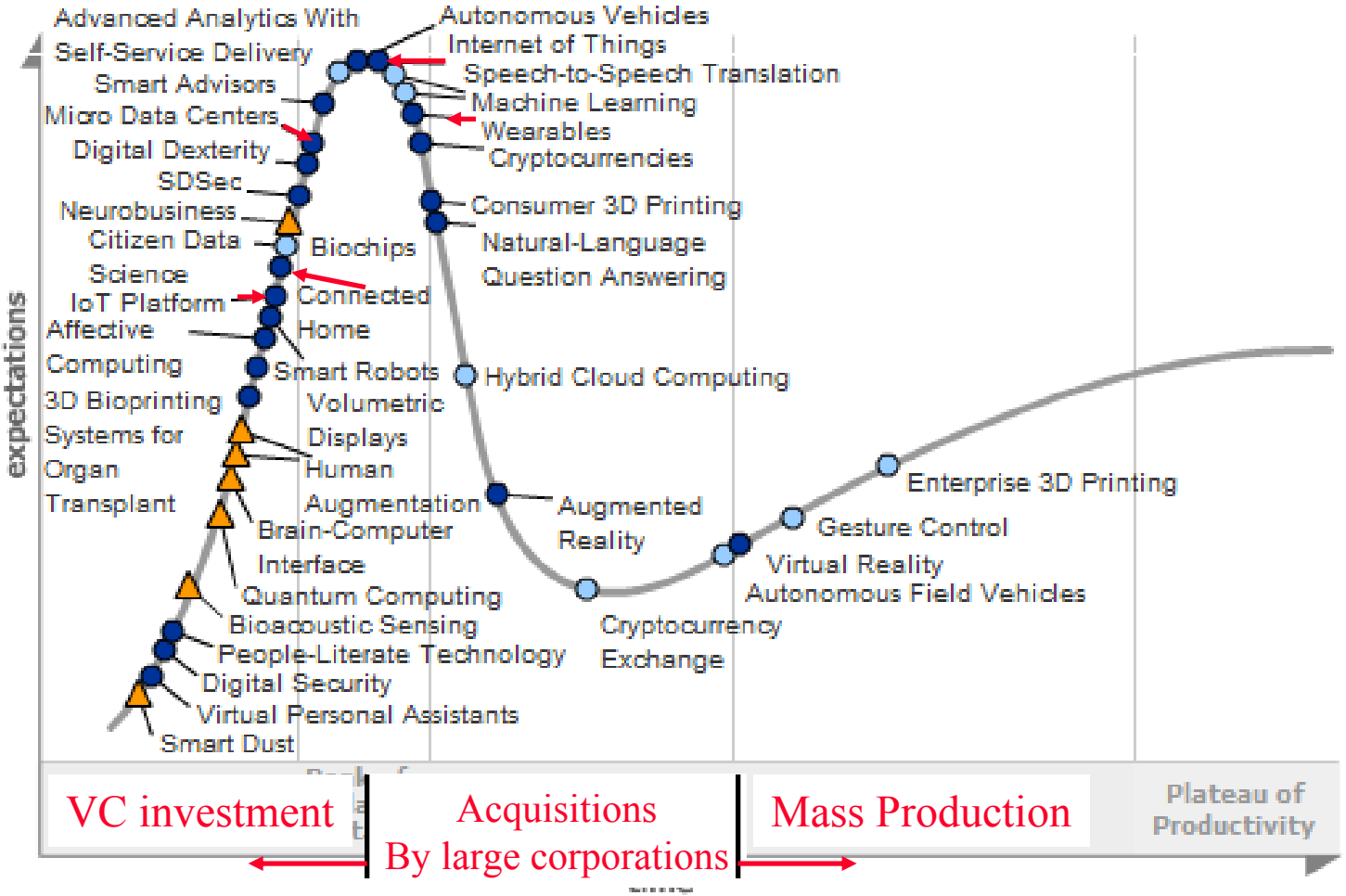
- Old: Smart = Can think ⇒ Computation
  = Can Recall ⇒ Storage
- Now: Smart = Can find quickly, Can Delegate
  ⇒ Communicate = Networking
- Smart Grid, Smart Meters, Smart Cars, Smart homes, Smart Cities, Smart Factories, Smart Smoke Detectors, …





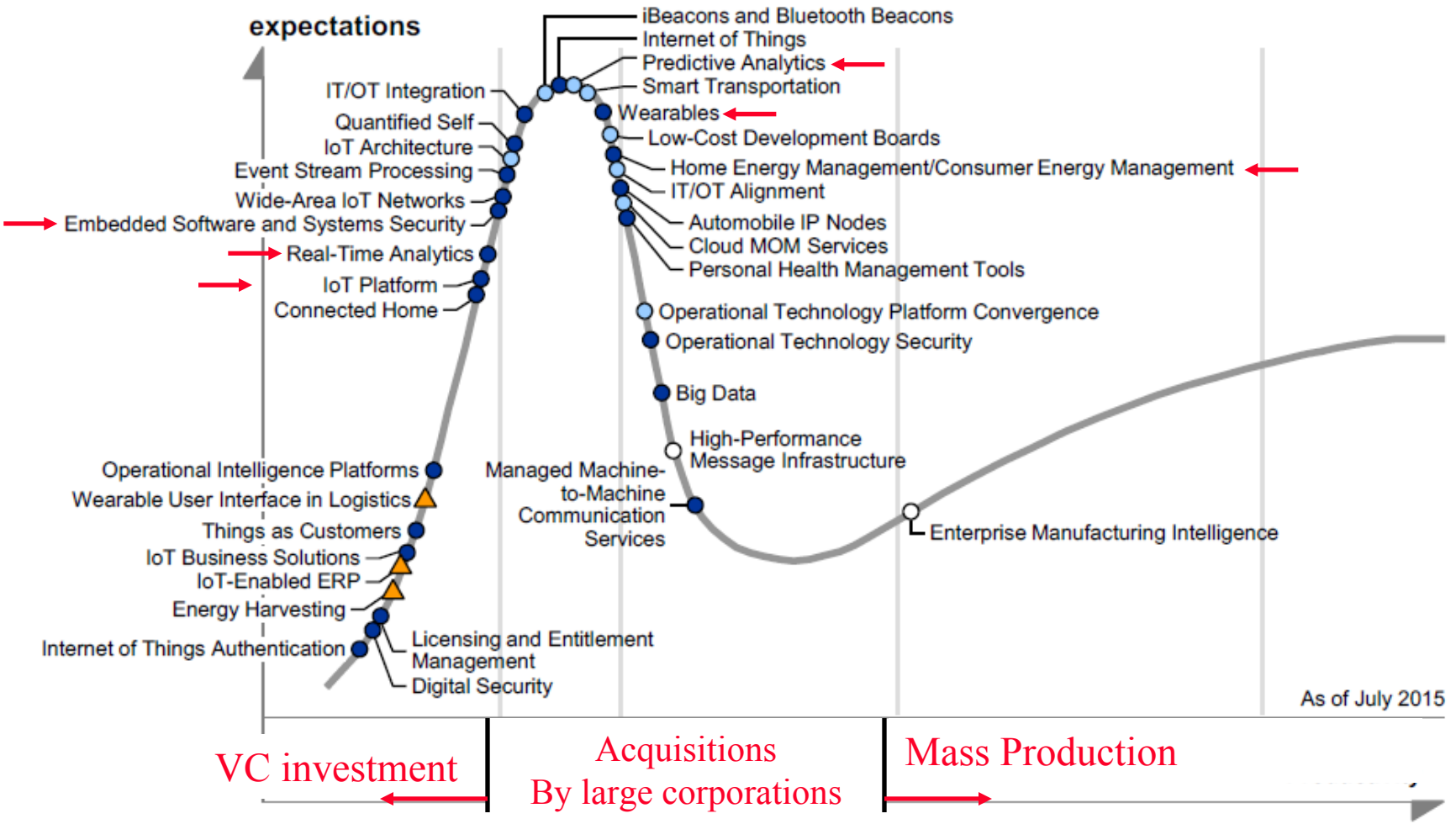
Not-Smart Smart

Gartner Hype Cycle 2015



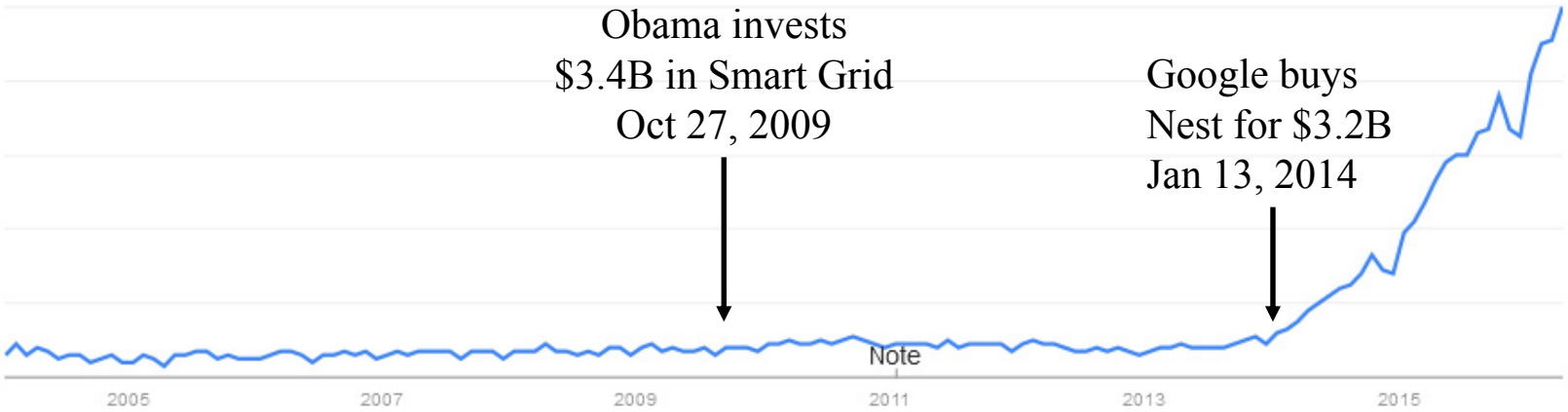
Ref: Gartner, "Hype Cycle for Emerging Technologies, 2015," July 2015, [Available to subscribers only], http://www.gartner.com/document/3100227?ref=QuickSearch&sthkw=hype%20cycle%202015&refval=156919648&qid=fe61993355944ace1c8c01ec2df676d9

Gartner's Hype Cycle For IoT 2015



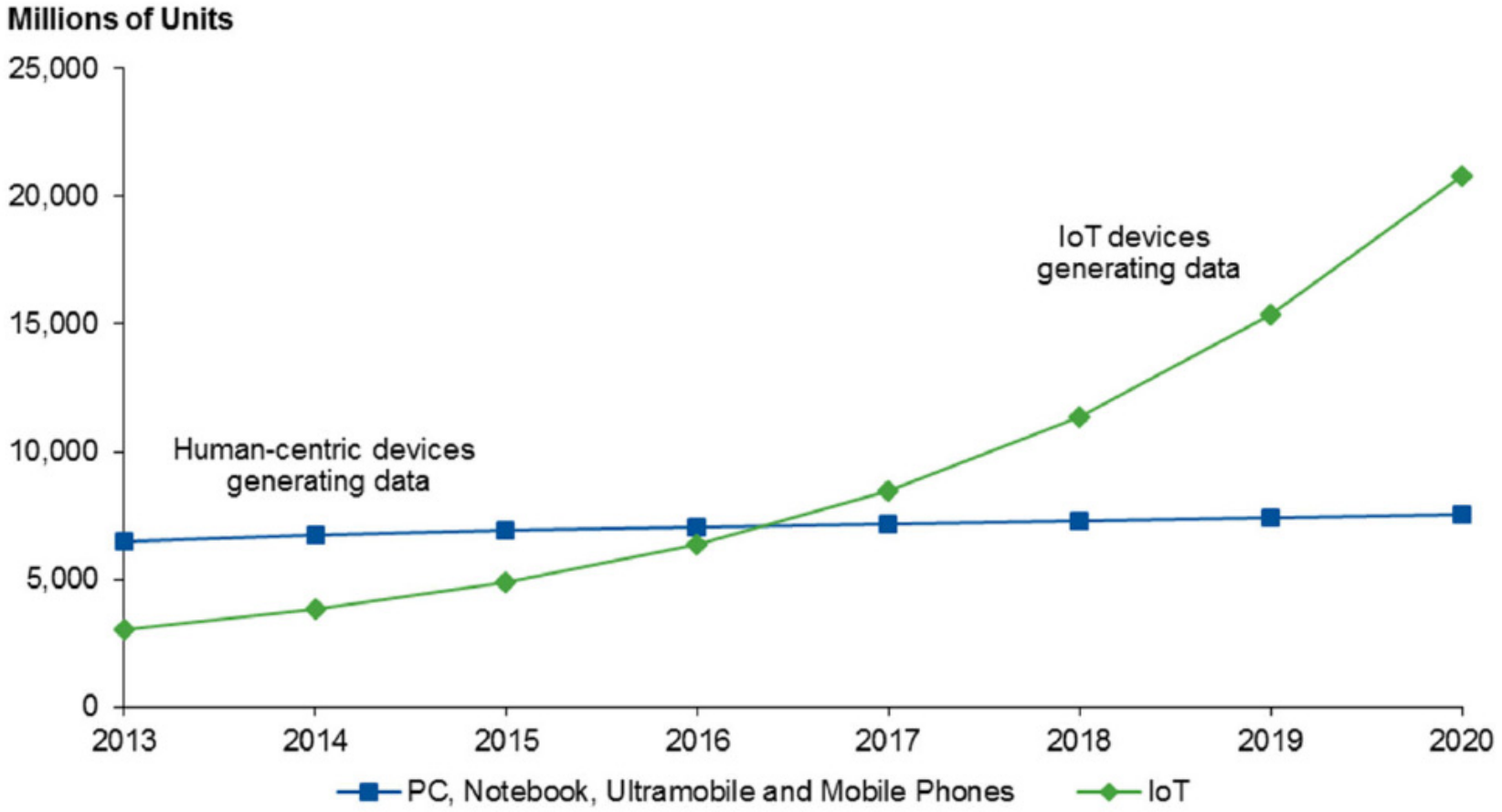
Ref: A Velosa, et al, "Hype Cycle for the Internet of Things, 2015" Gartner Report, G00272399, July 2015, 69 pp.

Google Trends



- Around for 10 years
- IERC-European Research Cluster on the Internet of Things funded under 7th Framework in 2009
  ⇒ "Internet of European Things"
- US interest started in 2009 w $3.4B funding for **smart grid** in American Recovery and Reinvestment Act of 2009

Computing vs. IoT



- 21 Billion devices by 2020

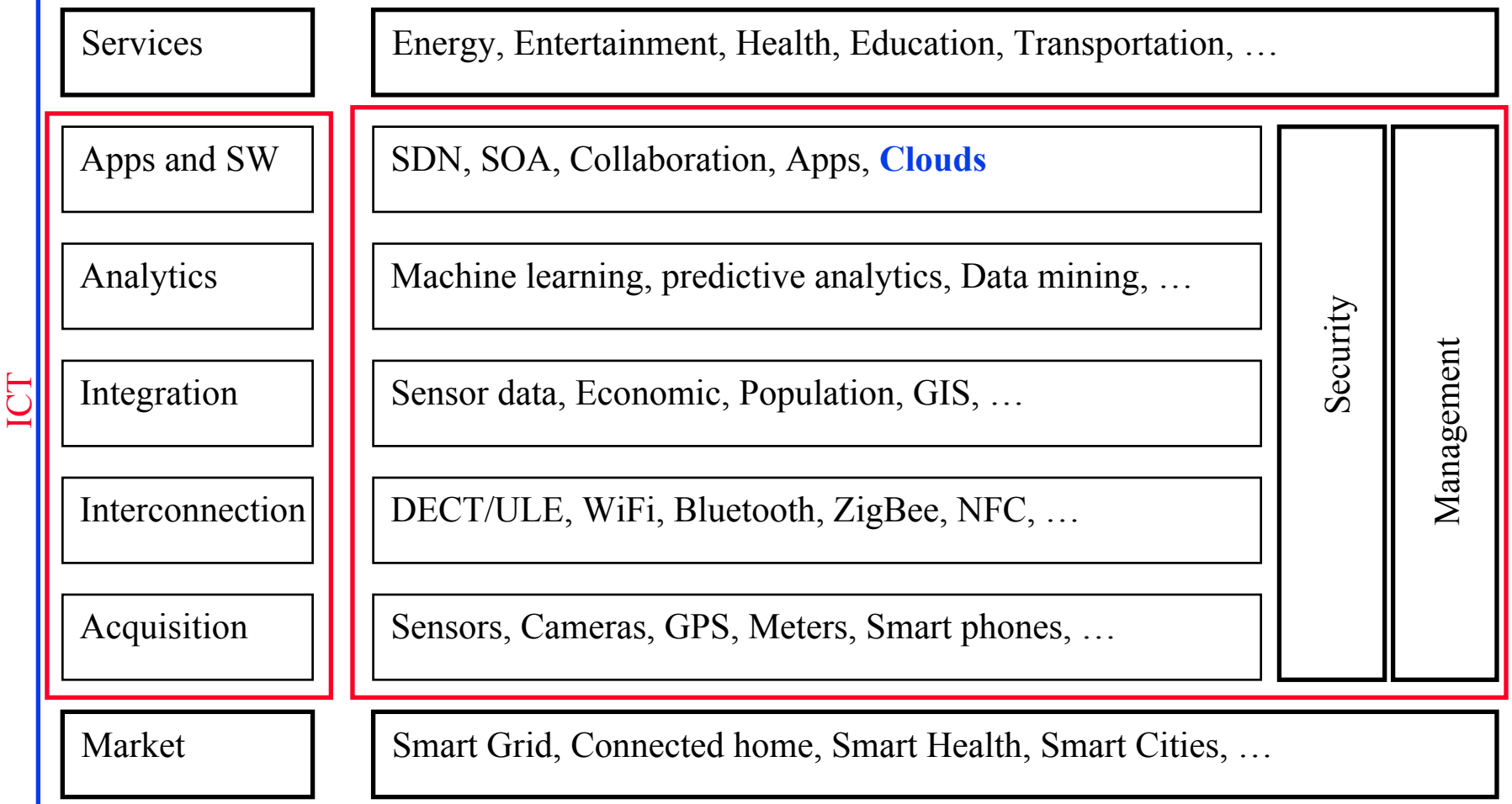
Ref: M. Moran, "Why the Internet of Things Will Dwarf Social (Big Data)," Gartner Report #G00289622, February 2016

IoT Business Opportunity

- $1.7 Trillion by 2020 - IDC
- $7.1 Trillion - Gartner
- $10-15 Trillion just for Industrial Internet – GE
- $19 Trillion – Internet of Everything - Cisco

Ref: http://www.forbes.com/sites/gilpress/2014/08/22/internet-of-things-by-the-numbers-market-estimates-and-forecasts/
http://www.forbes.com/sites/gilpress/2014/08/22/internet-of-things-by-the-numbers-market-estimates-and-forecasts/

A 7-Layer Model of IoT



Areas of Research for IoT

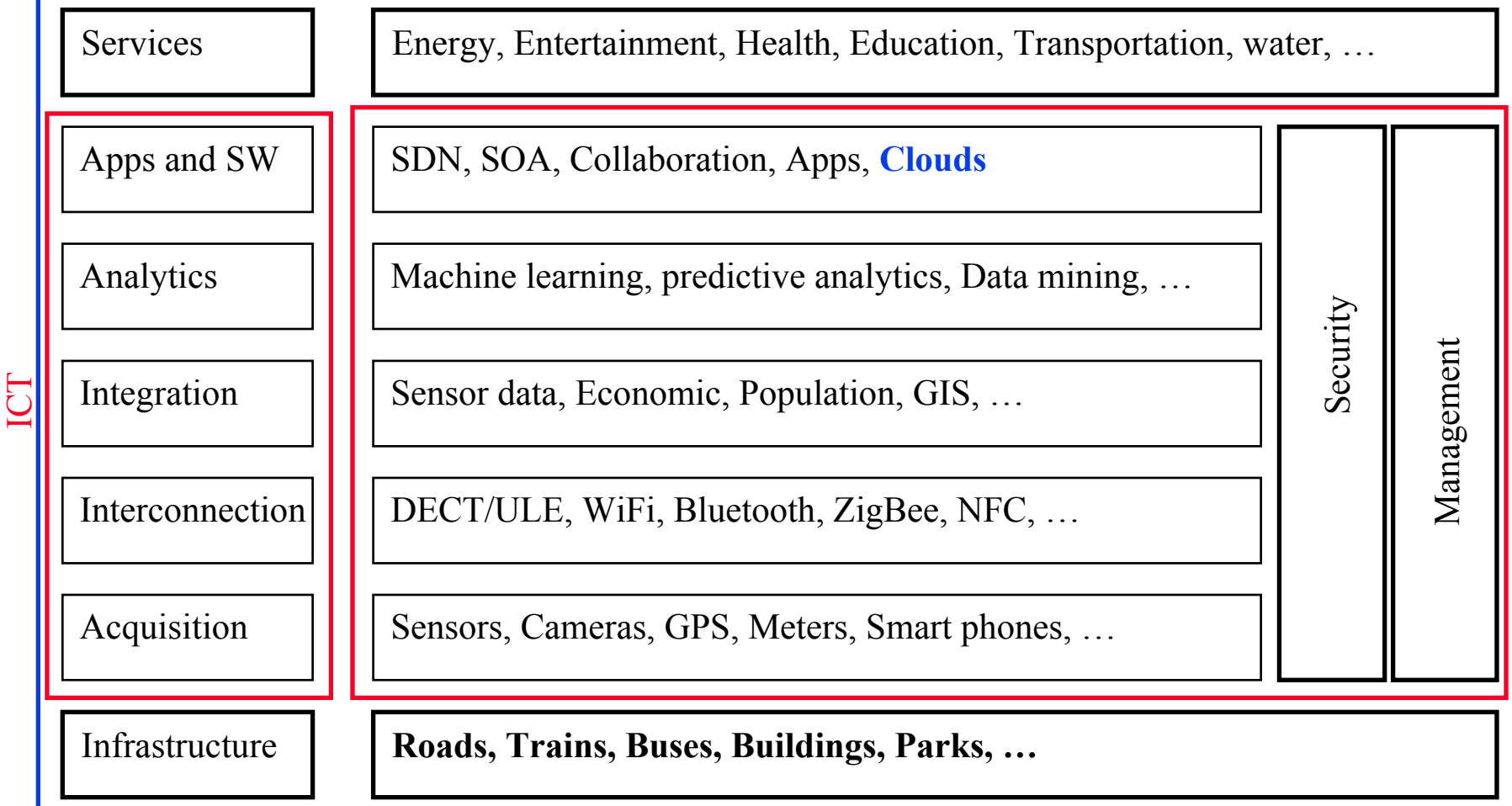
1. **PHY**: Smart devices, sensors giving real-time information, *Energy Harvesting*
2. **Datalink**: WiFi, Bluetooth, ZigBee, 802.11ah, … Broadband: DSL, FTTH, Wi-Fi, 5G, …
3. **Routing**: *Multiple interfaces,* Mesh networking, …
4. **Analytics**: Big-data, data mining, Machine learning, Predictive analytics, …
5. **Apps & SW**: SDN, SOA, Cloud computing, Web-based collaboration, Social networking, HCI, Event stream processing, …
6. **Applications**: Remote health, On-line education, on-line laboratories, …
7. **Security:** Privacy, Trust, Identity, Anonymity, …

IoT is a Data ($) Mine

Ref: https://www.pinterest.com/iofficecorp/humor/

Washington University in St. Louis http://www.cse.wustl.edu/~jain/talks/iots_tns.htm

A 7-Layer Model of Smart Cities



Why Are We Solving the Problem Now?

- $27.5 billion annual revenue in smart city technology by 2023
  $174 billion investment by 2023
- Cisco, Intel, Huawei, IBM, Fujitsu, SIEMENS are all selling ICT for smart cities
- India government will spend ~$7 billion for smart cities in the next five years

Ref: Navigant Research, "Smart Cities," https://www.navigantresearch.com/research/smart-cities

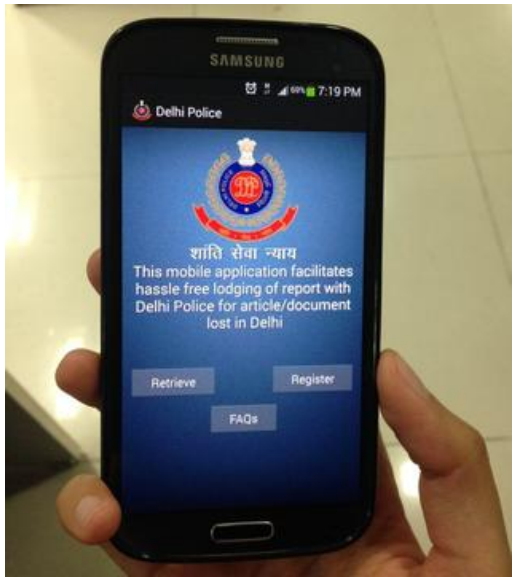
Smart Cities Research in US

- White House "Smart Cities Week" (Sep 15-18, 2015, Next: Sep 27-29, 2016)
- $40 M Research funding from NSF
  - Gigabit applications healthcare, energy, transportation, manufacturing, education and learning, and public safety.
  - Cyber physical systems
- Make Broadband construction faster:
  - Websites to list all federal assets available for broadband
  - Broadband installation during new road construction
- US Ignite Program: Multi-gigabit Applications ⇒ Uncompressed video

Ref: NSF, "Cultivating Smart and Connected Communities," http://nsf.gov/news/news_summ.jsp?cntn_id=136253
Smart City Week, http://www.smartcitiesweek.com/

Smart Services: Examples

- London's Datastore: Jobs, Waste, Crime, Visitors, …
  All open to public, http://data.london.gov.uk/
- New Songdo City, Incheon, South Korea: All city services available via Internet, video conferencing, http://www.songdo.com/
- Delhi police app to report crime
  55,000 reports in 6 months
- In Melbourne, All trees have been assigned ID numbers so that public can report tree problems, overgrown branches, fallen trees, etc.



Challenges

1. **Financing**: Self-sustaining ⇒ Revenue generating.
   Federal or state financing is just "seed" funding
   Private Partnerships ⇒ Revenue sharing or bartering
2. Ensuring **fairness** to all localities of a city
   ⇒ Private companies want the best revenue generating areas
3. **Public Trust**: in government, the data, and expect actions
   Lack of transparency ⇒ Waste of money on technologies
4. **Customization**: Every city is different.
   Private companies want to reuse their "one solution for all"
5. **Turnover**: Technology gets outdated every year or two
6. Digital **Disruption**
7. **Security and Privacy**

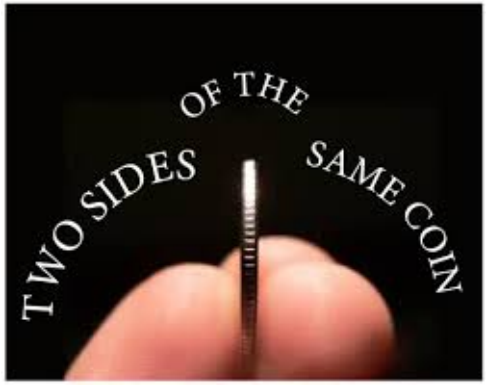
J. Bélissent, "Getting Clever About Smart Cities: New Opportunities Require New Business Models," Forester, Nov 2010, 33 pp., http://193.40.244.77/iot/wp-content/uploads/2014/02/getting_clever_about_smart_cities_new_opportunities.pdf

Public Trust

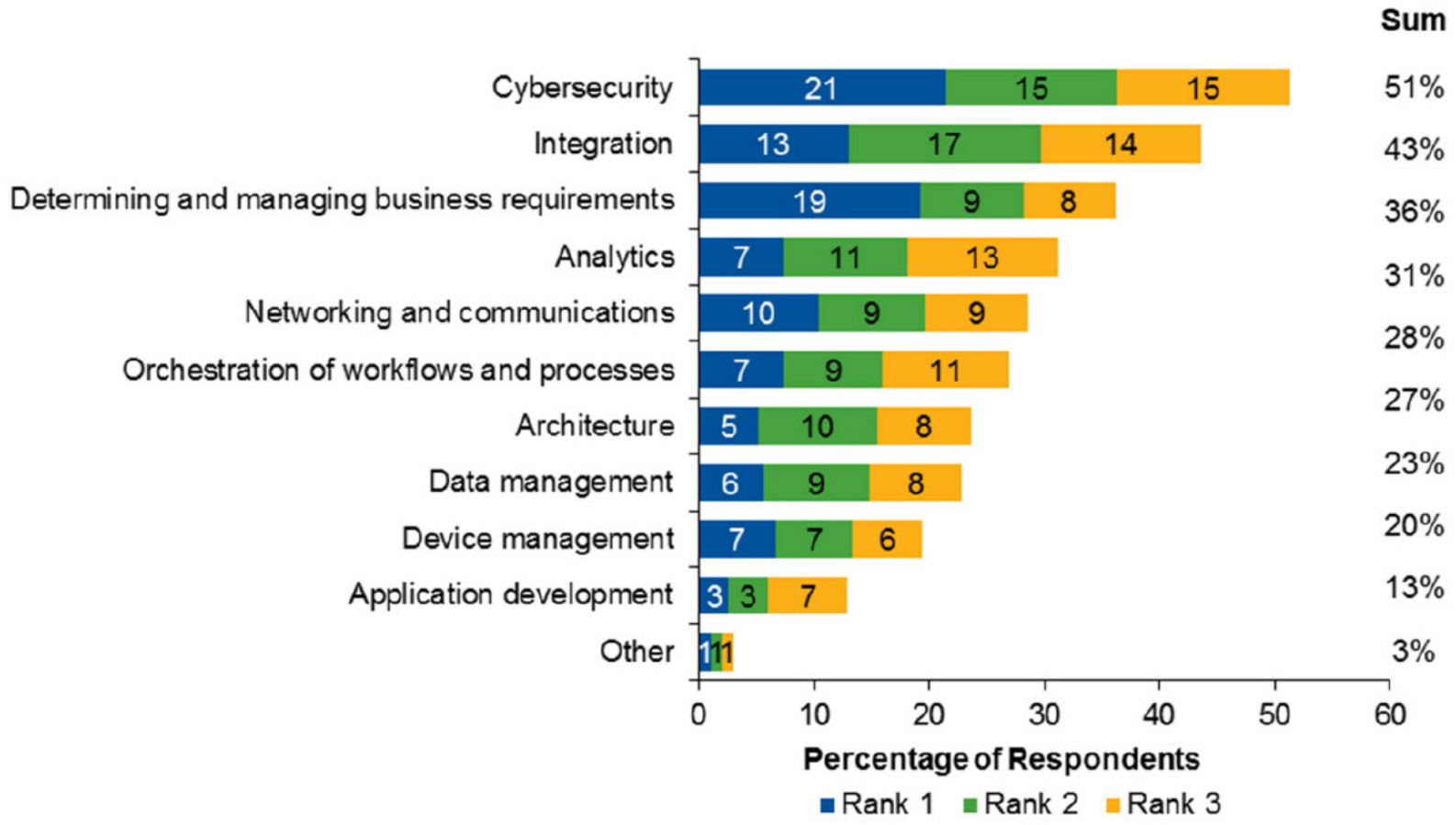
Ref: http://macleodcartoons.blogspot.in/2011_11_01_archive.html

Digital Disruptions

- New methods ⇒ Improvements ⇒ Disruption to old methods
- Automation ⇒ Better efficiency ⇒ What to do with those replaced
- Privatization, Automation, Change ⇒ Strikes



Top Inhibitors to the Adoption of the IoT



Ref: B. Lheurex, et al, "Survey Analysis: Users Cite Ambitious Growth and formidable Technical Challenges in IoT Adoption," Gartner Report #G00300127, March 2016,

Washington University in St. Louis http://www.cse.wustl.edu/~jain/talks/iots_tns.htm

IoT Security: Popular Approach

Ref: http://cloudtweaks.com/2011/08/the-lighter-side-of-the-cloud-the-migration-strategy/

Current IoT Security

- HP Study
  - 80% had privacy concerns
  - 70% lacked encryption
  - 60% had insecure updates
- Symantec Study:
  - 1/5th of Apps did not use SSL (Secure transfers)
  - None of the devices provided mutual (gateway) authentication
  - No lock-out/delaying measures against repeated attacks
  - Common web application vulnerabilities
  - Firmware upgrades were not encrypted

Ref: http://fortifyprotect.com/HP_IoT_Research_Study.pdf

Ref: M. Barcena and C. Wueest, "Insecurity in the Internet of Things," Symantec, March 2015,

Internet of Harmful Things

Imagine, as researchers did recently at Black Hat, someone hacking your connected toilet, making it flush incessantly and closing the lid repeatedly and unexpectedly.

Ref: http://www.computerworld.com/article/2486502/security0/worm-may-create-an-internet-of-harmful-things--says-symantec--take-note--amazon-.html

Security ≠ AES-128

- CIA = Confidentiality, Integrity, Availability
  = Encryption + Message Authentication Code + Denial of Service Prevention
- Use of AES-128 does not guarantee security.
- Insecurity:
  - How strong is the key?
  - Where the key is stored?
  - Bugs in system code
  - Backdoors

DEFCON 2015

DEFCON 2015 (Cont)

- Hacking a Linux rifle
- Hacking smart safes
- Wirelessly steal cars
- Hack a Tesla
- Hack ZigBee
- Hacking IoT baby monitors
- Hacking FitBit Aria
- Cracking crypto currency
- Hack out of home detention
- Insteon's false security
- Hacking RFID, NFC
- DARPA Cyber Grand Challenge $2M

Ref: https://www.ethicalhacker.net/features/opinions/first-timers-experience-black-hat-defcon

Door Locks Insecurity

- **Onity Door Locks**:
  - Used on hotel doors with magnetic strips
  - Information is encrypted using a hotel-specific secret key
  - **Programming port** on the bottom
  - Security Key can be read through programming port
  - Firmware update not possible ⇒ Replace hardware
- **Sigma Design's Z-Wave Door Locks**:
  - Z-Force tool can monitor traffic and have the lock accept a an arbitrary encryption key
- **Kwikset Kevo Door Locks**:
  - **Password** can be reset by email
  - Hijacked email addresses and phishing attack

Ref: N. Dhanjani, "Abusing the Internet of Things: Blackouts, Freakouts, and Stakeouts," O'Reilly, 2015, ISBN: 978-1-491-90233-2

Attack Surface

1. **IoT Devices**
2. **IoT wireless access technology**: DECT, WiFi, Z-wave, …
3. **IoT Gateway**: Smart Phone
4. **Home LAN**: WiFi, Ethernet, Powerline, …
5. **IP Network**: DNS, Routers, …
6. **Higher-layer Protocols**
7. **Cloud**
8. **Management Platform**: Web interface
9. **Life Cycle Management**: Booting, Pairing, Updating, …

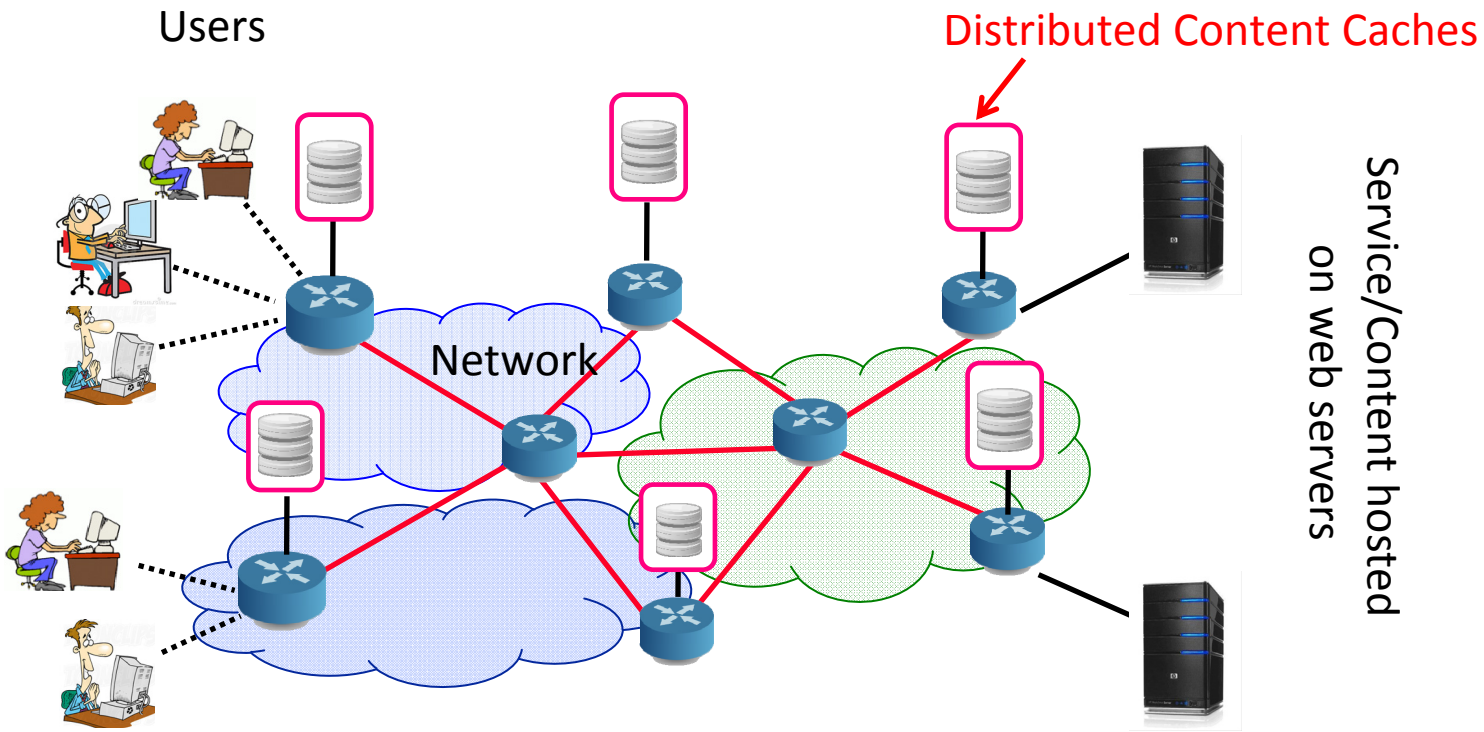
Smart City Insecurity

- **Smart Court House**: Placer county courthouse accidently summoned 1200 people to jury duty on a morning in May 2012 causing traffic jams
- **Smart Metro**: Bay Area Rapid Transit (BART) was shut down by a technical problem affecting 500 to 1000 passengers on 19 trains (November 2013)
- **Smart Electricity**: 55 Million people in Northeast USA lost electric power due to a software bug
- Not marking a pipeline on the map lead to a gas pipe line explosion and fire in Johnson County, Texas by workers installing electrical lines
- Nation states and cyber terrorists know how to make use of public data ⇒ **Smart Wars**

Ref: C. Cerrudo, "Hacking smart cities," RSA Conference 2015, http://www.rsaconference.com/writable/presentations/file_upload/hta-t10-hacking-smart-cities_final.pdf

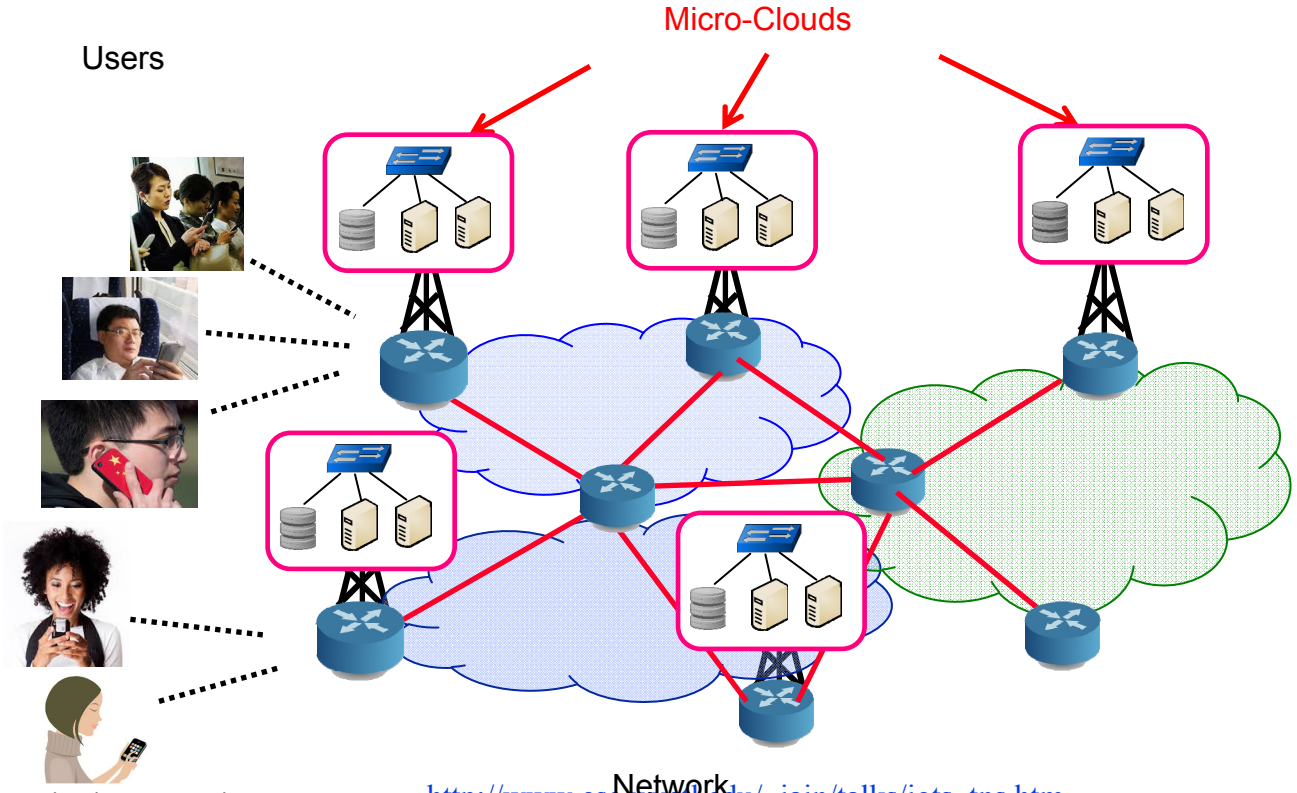
Past: Data in the Edge

- To serve world-wide users, latency was critical and so the data was replicated and brought to edge



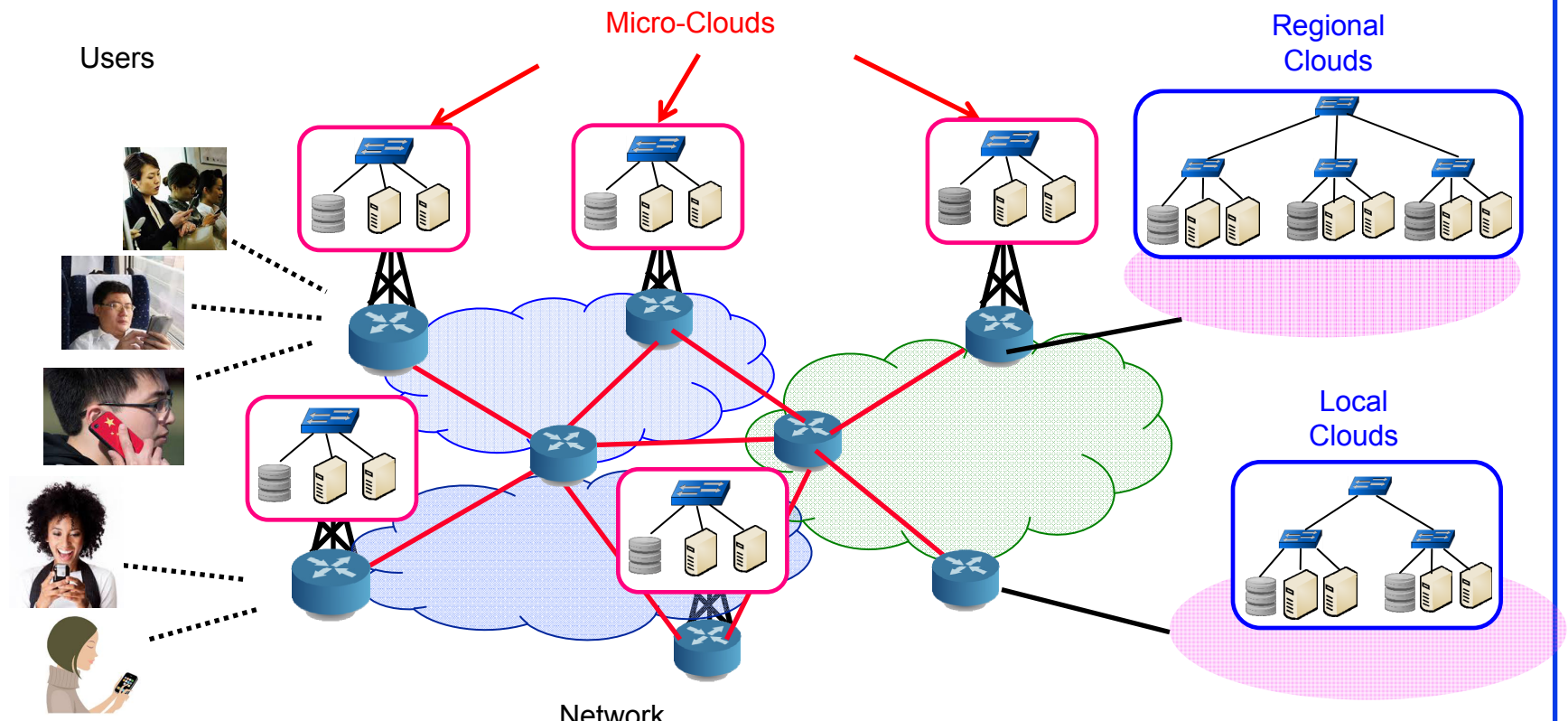
Trend: Computation in the Edge

- To service mobile users/IoT, the computation needs to come to edge ⇒ Micro-cloud on the tower
  ⇒ Mobile-Edge Computing



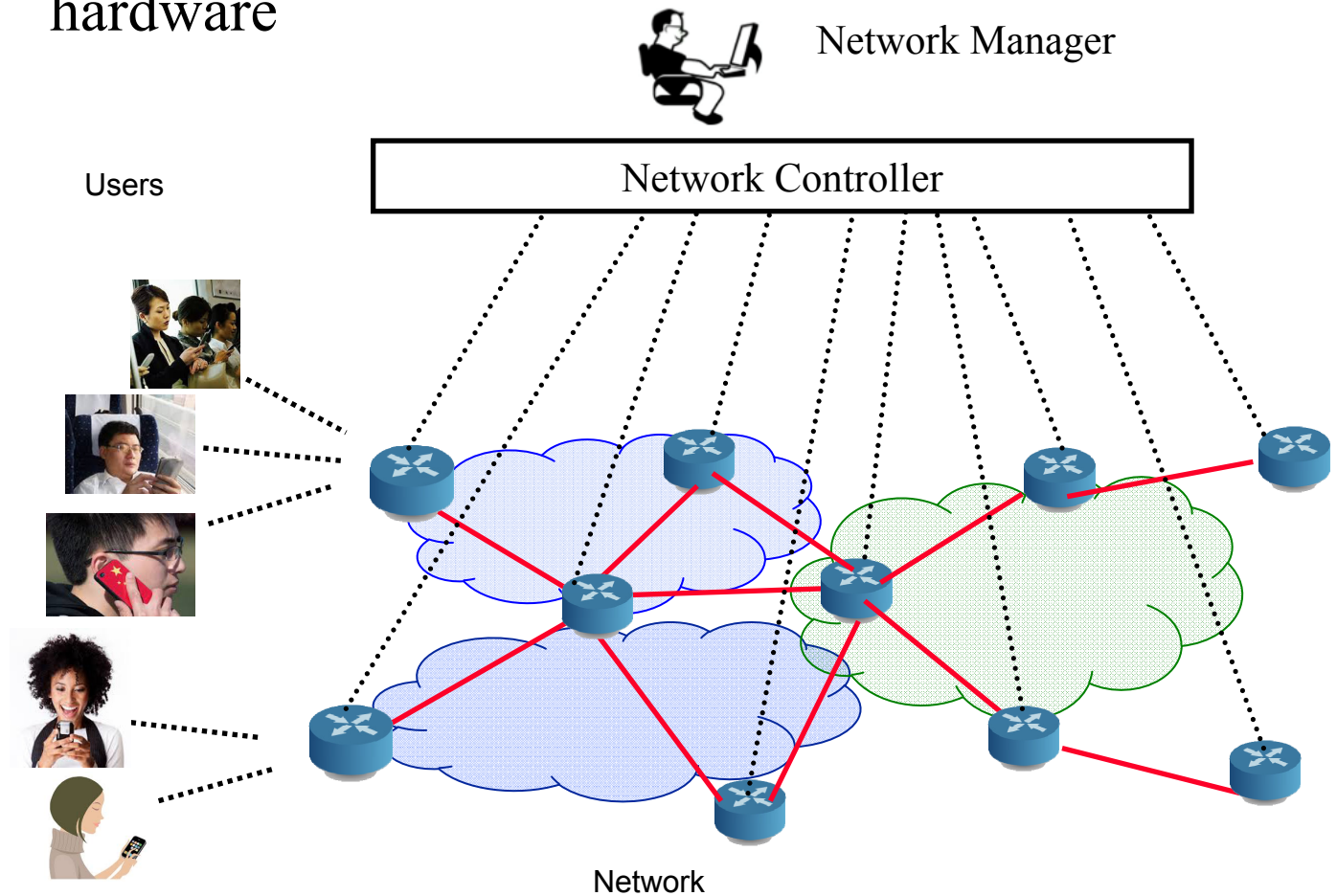
Trend: Multi-Cloud

- Larger and infrequent jobs serviced by local and regional clouds ⇒ Fog Computing



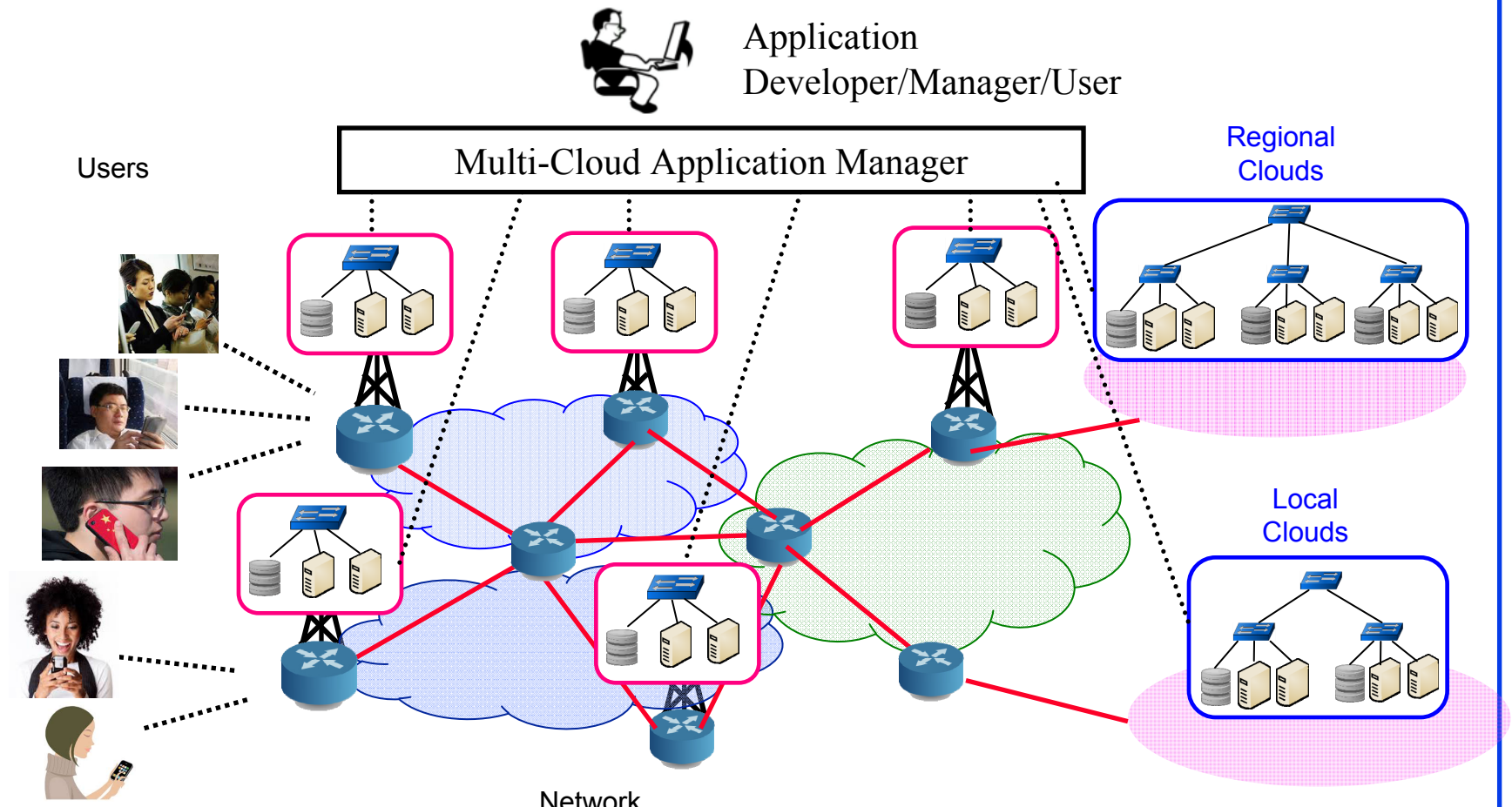
Past: Software Defined Networking

- Network can be managed w/o worrying about individual device hardware

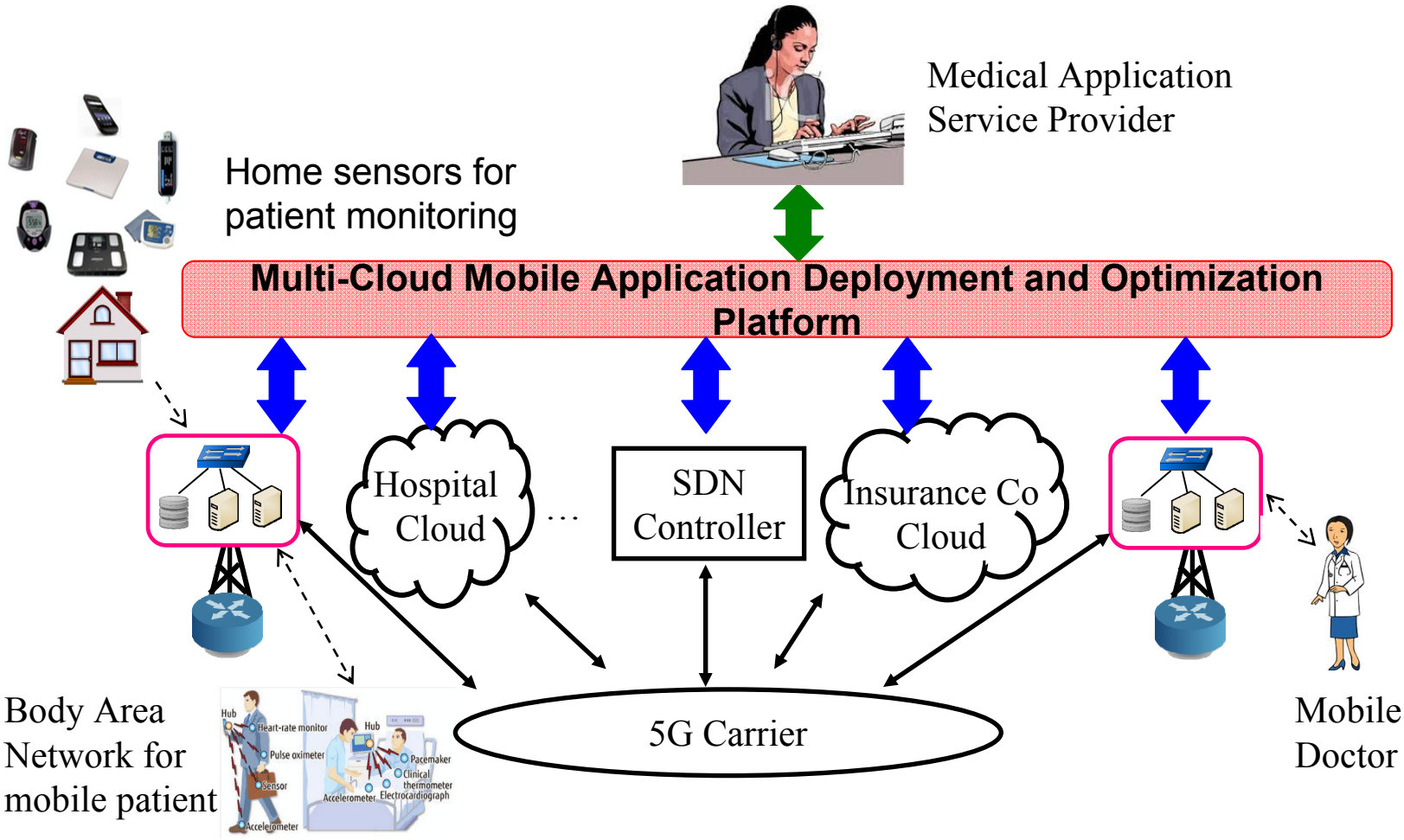


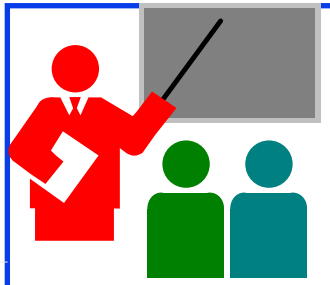
Trend: Software Defined Multi-Cloud Application Delivery

- Cloud MOM (message oriented middleware)



Mobile Healthcare Use Case





Summary

1. Smart ≠ High-Speed Computation, Smart ≠ Big Data Storage, Smart = Networked
2. IoT/Smart Cities research areas are easy via the 7-layer model They have brought in research issues in every layer: Sensors, datalink, routing, applications, analytics.
3. Numerous challenges: Sustainable partnerships, Digital disruption, fast technology turnover, trust. Security and privacy are most important issues
4. Computation is moving to the Edge ⇒ Fog Computing ⇒ Multi-Cloud/Inter-Cloud
5. Our MCAD abstracts/virtualizes the cloud interfaces and allows automated management of security and other policies of multi-cloud applications

Recent Talks on IoT/Smart Cities

- Raj Jain, "**Internet of Things: Research Issues**," NSF Applications and Services Workshop, January 27, 2016, http://www.cse.wustl.edu/~jain/talks/iot_nsf.htm
- Raj Jain, "**Internet of Things: Research Challenges and Issues**," Keynote at the Internet of Things World Forum, Research and Innovation Symposium, Dubai, December 5-6, 2015, http://www.cse.wustl.edu/~jain/talks/iotwrld.htm
- Raj Jain, "**Internet of Things Security**," Keynote at STLCybercon 2015, University of Missouri, St. Louis, November 20, 2015, http://www.cse.wustl.edu/~jain/talks/iots_um.htm
- Raj Jain, "**Smart Cities: Technological Challenges and Issues**," IEEE CS Keynote at 21st Annual International Conference on Advanced Computing and Communications (ADCOM) 2015, Chennai, India, September 19, 2015, Chennai, India, September 18, 2015, http://www.cse.wustl.edu/~jain/talks/smrtcit.htm
- Raj Jain, "**Internet of Things: Challenges and Issues**," **IEEE CS Keynote** at 20th Annual Conference on Advanced Computing and Communications (ADCOM 2014), Bangaluru, India, September 19, 2014, http://www.cse.wustl.edu/~jain/talks/iot_ad14.htm

Recent Papers on Multi-Cloud

- Subharthi Paul, Raj Jain, Mohammed Samaka, Jianli Pan, "Application Delivery in Multi-Cloud Environments using Software Defined Networking," Computer Networks Special Issue on cloud networking and communications, Available online 22 Feb 2014, http://www.cse.wustl.edu/~jain/papers/comnet14.htm
- Raj Jain and Subharthi Paul, "Network Virtualization and Software Defined Networking for Cloud Computing - A Survey," IEEE Communications Magazine, Nov 2013, pp. 24-31, http://www.cse.wustl.edu/~jain/papers/net_virt.htm
- Subharthi Paul, Raj Jain, Mohammed Samaka, Aiman Erbaud, "Service Chaining for NFV and Delivery of other Applications in a Global Multi-Cloud Environment," ADCOM 2015, Chennai, India, September 19, 2015, http://www.cse.wustl.edu/~jain/papers/adn_in15.htm
- Deval Bhamare, Raj Jain, Mohammed Samaka, Gabor Vaszkun, Aiman Erbad, "Multi-Cloud Distribution of Virtual Functions and Dynamic Service Deployment: OpenADN Perspective," Proceedings of 2nd IEEE International Workshop on Software Defined Systems (SDS 2015), Tempe, AZ, March 9-13, 2015, 6 pp. http://www.cse.wustl.edu/~jain/papers/vm_dist.htm

Acronyms

- 4G — Fourth Generation
- 5G — Fift Generation
- 6TiSCH — IPv6 over Time Slotted Channel Hopping Mode of IEEE 802.15.4e
- ADCOM — Advanced Computing and Communications
- AES-128 — Advanced Encryption Standard
- AMQP — Advanced Message Queuing Protocol
- ANSI — American National Standards Institute
- ANT — A proprietary open access multicast wireless sensor network
- ANT+ — Interoperability Function added to ANT
- BS — British Standard
- BSI — British Standards Institute
- CARP — Channel-Aware Routing Protocol
- CD — Committee Draft
- CEN — European Committee for Standardization
- CENELEC — European Committee for Electro technical Standardization
- CG — Coordination Group

Acronyms (Cont)

CIA	Confidentiality, Integrity, Availability
CoAP	Constrained Application Protocol
CoRE	Constrained RESTful Environment
CORPL	Cognitive RPL
CS	Computer Society (IEEE)
DARPA	Defense Advance Research Project Agency
DASH-7	Named after last two characters in ISO 18000-7
DDS	Data Distribution Service
DECT	Digital Enhanced Cordless Telephone
DECT/ULE	Digital Enhanced Cordless Telephone with Ultra Low Energy
DEFCON	d-e-f conference (named after alphabets d, e, f)
DIN	Deutsches Institut für Normung (German Institute for Standardization)
DIS	Draft International Standard
DNS	Domain Name System
DSL	Digital Subscriber Line

Acronyms (Cont)

- DTLS Datagram Transport Layer Security
- DTS Draft Technical Specification
- ECC Error Correcting Code
- EDSA Embedded Device Security Assurance
- ETSI European Telecommunications Union
- FG-SSC Focus group on smart sustainable cities
- FTTH Fiber to the home
- FTTx Fiber to the X
- GB Gigabyte
- GDP Gross Domestic Production
- GE General Electric
- GIS Geographical Information Systems
- GP Green PHY
- GPS Global Positioning System
- HCI Human Computer Interface
- HMAC Keyed-Hash Message Authentication Code

Acronyms (Cont)

- HP Hewlett Packard
- HTTP Hyper Text Transfer Protocol
- ICS Industrial Control Systems
- ICT Information and Communications Technology
- ID Identification
- IDC International Data Corporation
- IDs Identifiers
- IEC International Engineering Council
- IEC/SEG IEC Systems Evaluation Group
- IEEE Institution of Electrical and Electronic Engineers
- IETF Internet Engineering Task Force
- IFC Industry Foundation Classes
- IMS IP Multimedia System
- IoT Internet of Things
- IP Internet Protocols
- IQ Intelegence Quotient

Acronyms (Cont)

- IRTF — Internet Research Task Force
- ISA — International Society of Automation
- ISBN — International Standard Book Number
- ISO — International Standards Organization
- IT — Information Technology
- ITU-T — International Telecommunications Union - Telecommunication Standardization Sector
- JTC — Joint Technical Committee
- KPI — Key Performance Indicator
- LAN — Local Area Network
- LoRaWAN — Long Range Wide Area Network
- LowPAN — Low Power Personal Area Network
- LTE — Long-Term Evolution
- MCAD — Multi-Cloud Application Delivery
- MHz — Mega Hertz
- MO — Missouri
- MOM — Message Oriented Middleware

Acronyms (Cont)

- MQTT Message Queue Telemetry Transport
- NFC Near Field Communication
- NIST National Institute of Technology
- NSF National Science Foundation
- OAuth Open Protocol of Secure Authorization
- OpenADN Open Application Delivery Networking
- OS Operating System
- PAS Publicly Available Specification
- PD Published Document
- PHY Physical Layer
- PKI Public Key Infrastructure
- RFC Request for Comment
- RFID Radio Frequency Identifier
- RoW Rest of the World
- RPL Routing Protocol for Low Power and Lossy Networks
- RSA Rivest, Shamir, and Adleman

Acronyms (Cont)

- RTS Road traffic safety
- SASL Simple Authentication and Security Layer
- SC Smart community
- SDLA Requirements for Security Development Lifecycle Assurance
- SDN Software Defined Networking
- SDS Software Defined Systems
- SEG System Evaluation Group
- SG5 Study Group 5
- SMACK Simple Mandatory Access Control Kernel for Linux
- SOA Service oriented Architecture
- SSA Software Security Assurance
- SSC Smart and Sustainable Cities and
- SSCC-CG Smart and Sustainable Cities and Communities Coordination Group
- SSL Secure Session Layer
- SW Software
- TC Technical Committee

Acronyms (Cont)

- TCG Trusted Computing Group
- TCP Transmission Control Protocol
- TLS Transport Level Security
- TMB Technical Management Board
- TNC Trusted Network Connect
- TPM Trusted Platform Module
- TR Technical Report
- TS Technical Specification
- TV Television
- UDP User Datagram Protocol
- ULE Ultra Low Energy
- US United States
- USA United States of America
- VC Virtual Circuit
- VDE Association for Electrical, Electronic & Information Technologies
- VM Virtual Machine

Acronyms (Cont)

- WAN Wide Area Network
- WCCD World Council on City Data
- WG Working Group
- WiFi Wireless Fidelity
- WiMAX Worldwide Interoperability of Microwave Access
- WirelessHART Wireless Highway Addressable Remote Transducer Protocol

Scan This to Download These Slides

Slides at:

bit.ly/jain_iots