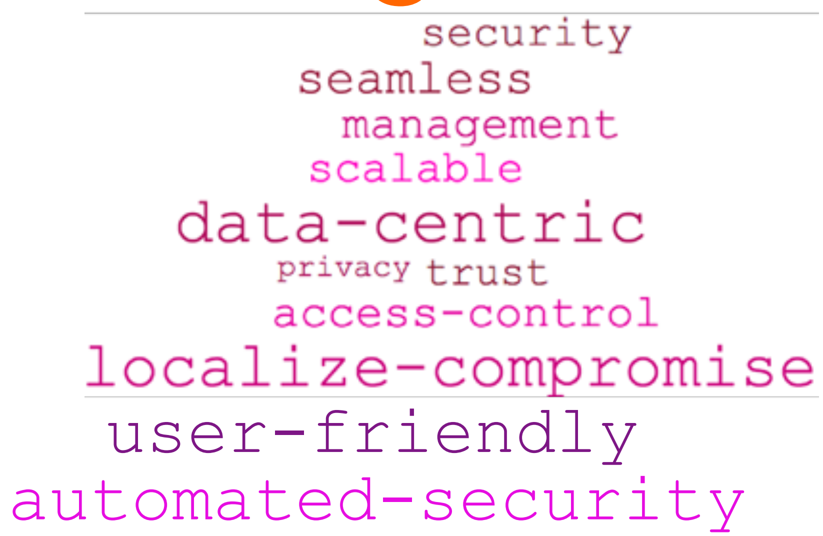
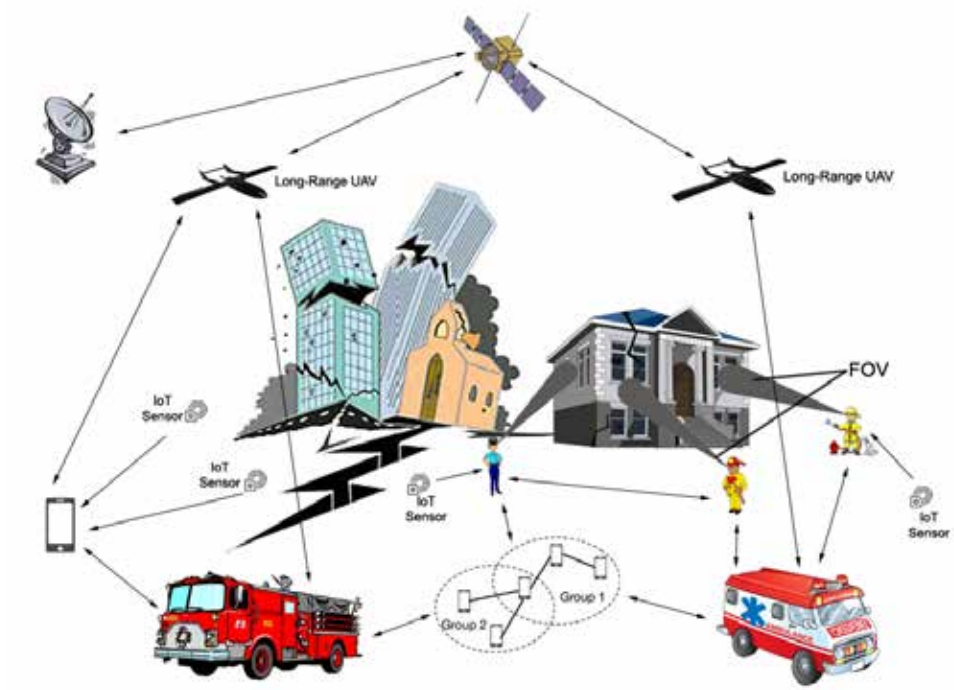
Secure and Private Wireless-Edge Networking via Named Data



Jay (Satyajayant) Misra, misra@cs.nmsu.edu

Part of the ICE-AR team, led by Prof. Lixia Zhang

Use-cases for ICE-AR



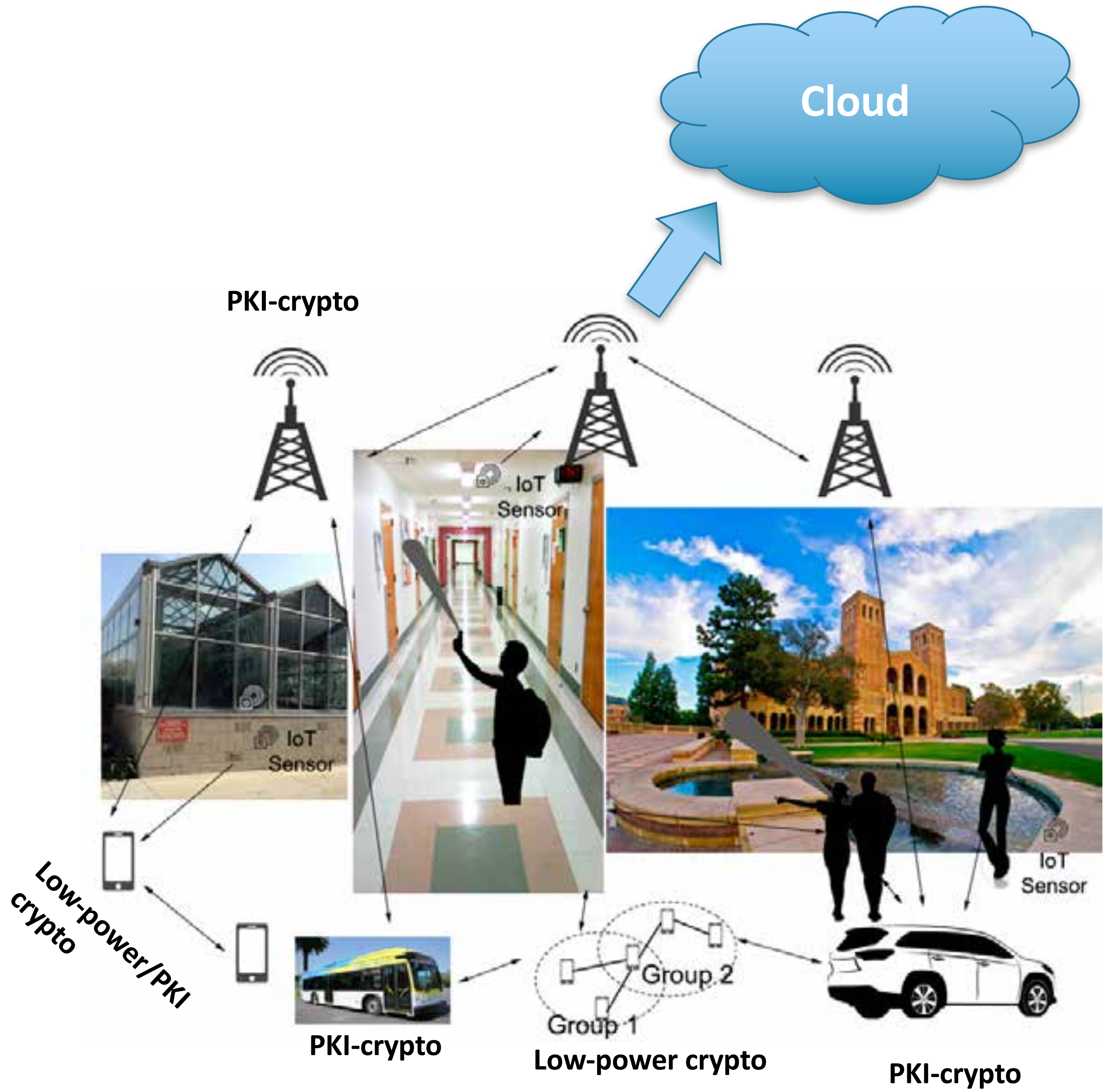
Campus Scenario → Disaster Scenario

Infrastructure and Compute Support, Trusted devices

ICE-AR: Minimum effort transition possible

Disrupted communication, diverse agencies, wide-trust spectrum

Diverse Device Classes and Capabilities



Powerful Devices
API, Accelerator, Wireless AP, BS (cells: femto, micro, etc.), First-responder vehicles

PKI; Acceleration; GPUs.

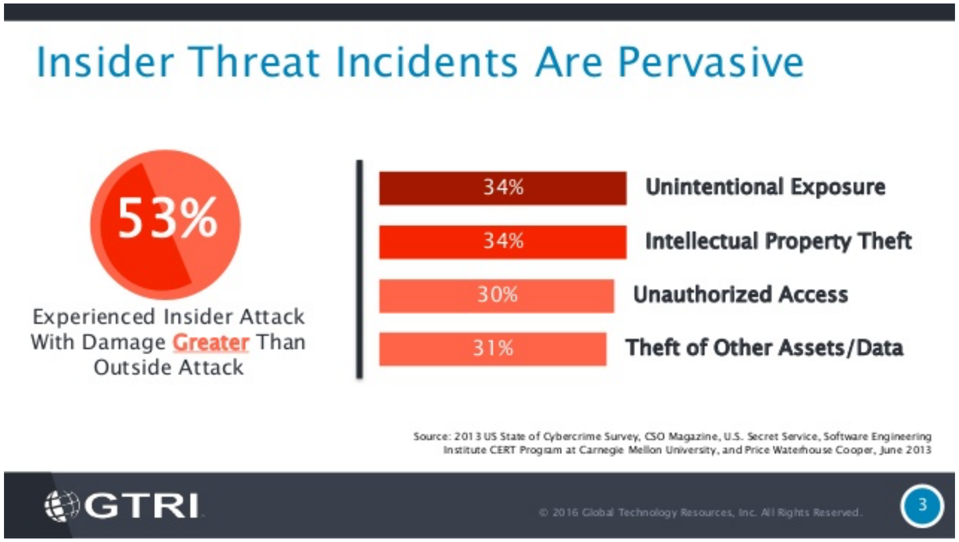
Somewhat Constrained Devices
Smart phones, Tablets, Head-mounted displays

PKI, Symmetric Key Infrastructure; Some acceleration

Low-power Devices
IoT devices, sensors, etc.

Symmetric Key; Low-cost hashing, Hash-chains

Threat Model



Insider Attack

Valid Identities, Certificates, Namespaces, Routes
(*Trusted (students, faculty); Semitrusted (guests of trusted entity); Untrusted (visitors)*)

Fake data, hijacking name-prefix;
sinkhole, blackhole, wormhole, DoS/DDoS

Outsider Attack

Only guest identity/certs (at best), no pervasive routing

Passive monitoring and traffic analysis, jamming to disrupt communications, probing network structure

Cannot perform DoS/DDoS as does not have credentials to sign packets

NDN: "intrinsic data provenance/ authenticity"

Conceptually simple

Realization is a giant research task

No concept of identity of netizens

Open env., large scale cert. distribution not feasible

- Name-based solutions

Scalable Trust Management

Data Security & Access Control

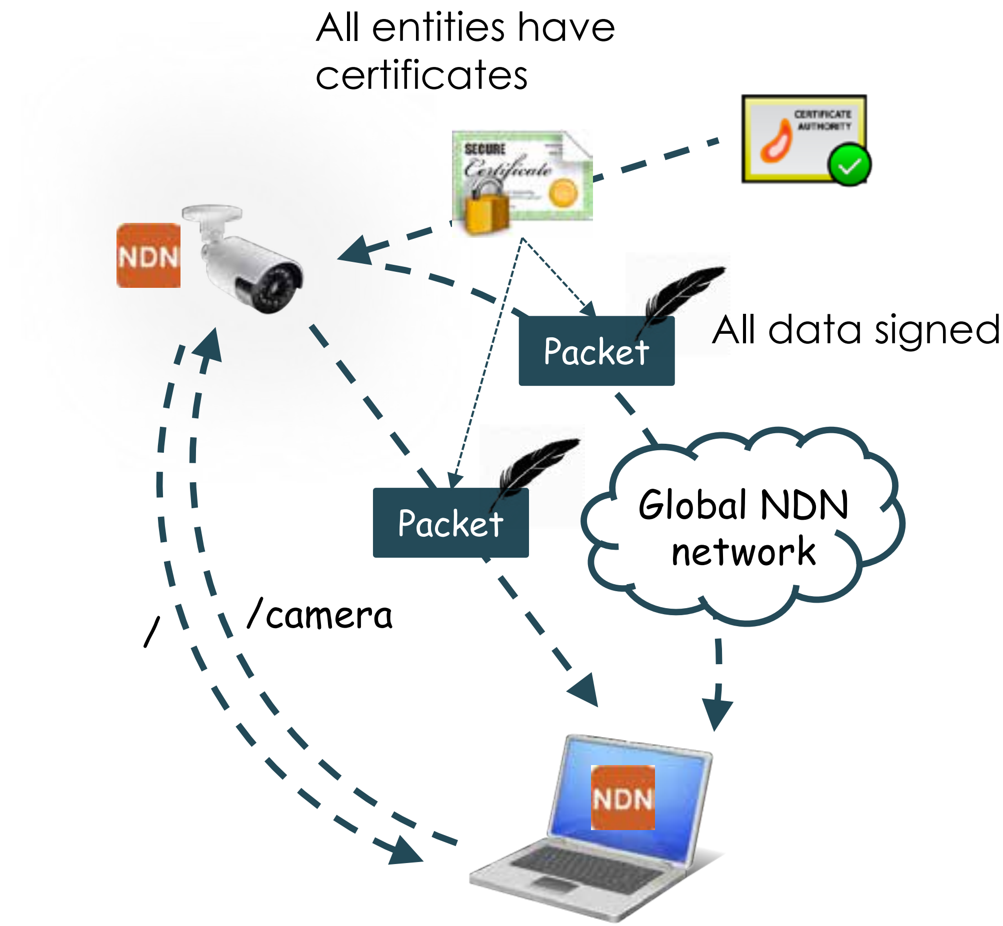
Location-based identity

Acceleration for scalability at line-speed

"On the Internet, nobody knows you're a dog."

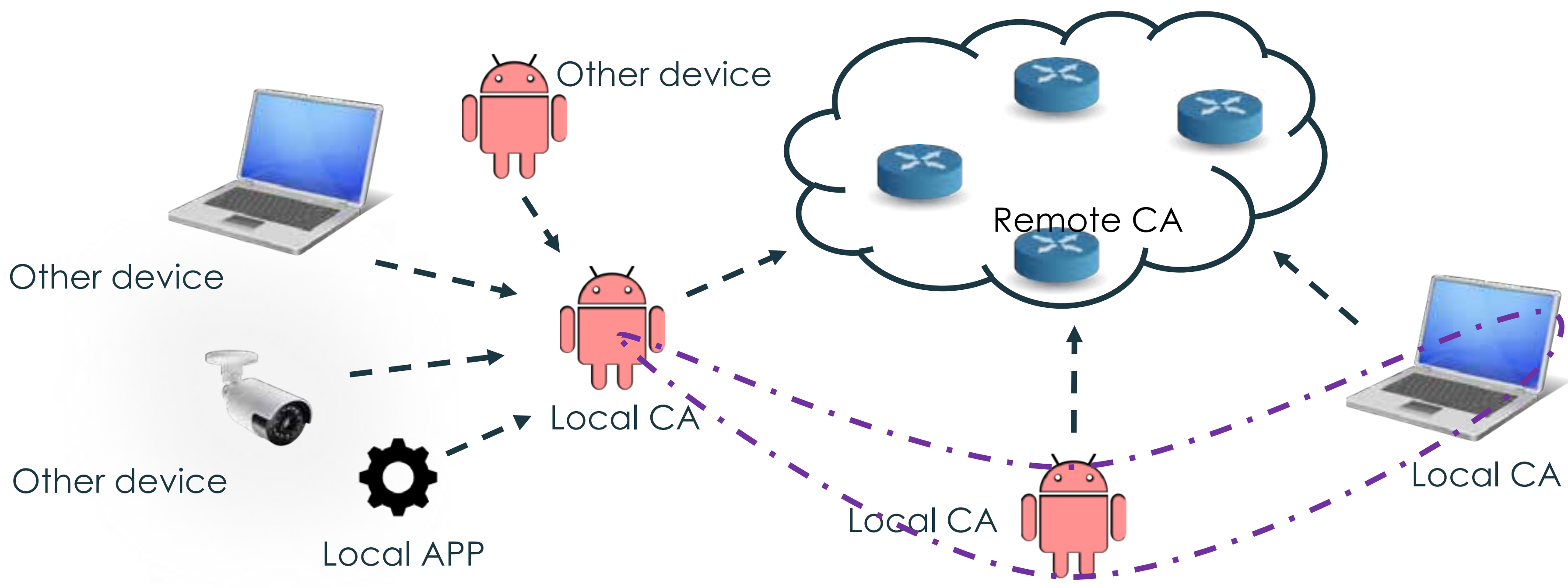
Image Credit: https://en.wikipedia.org/wiki/On_the_Internet,_nobody_knows_you%27re_a_dog

Example: A camera publishing data into the network



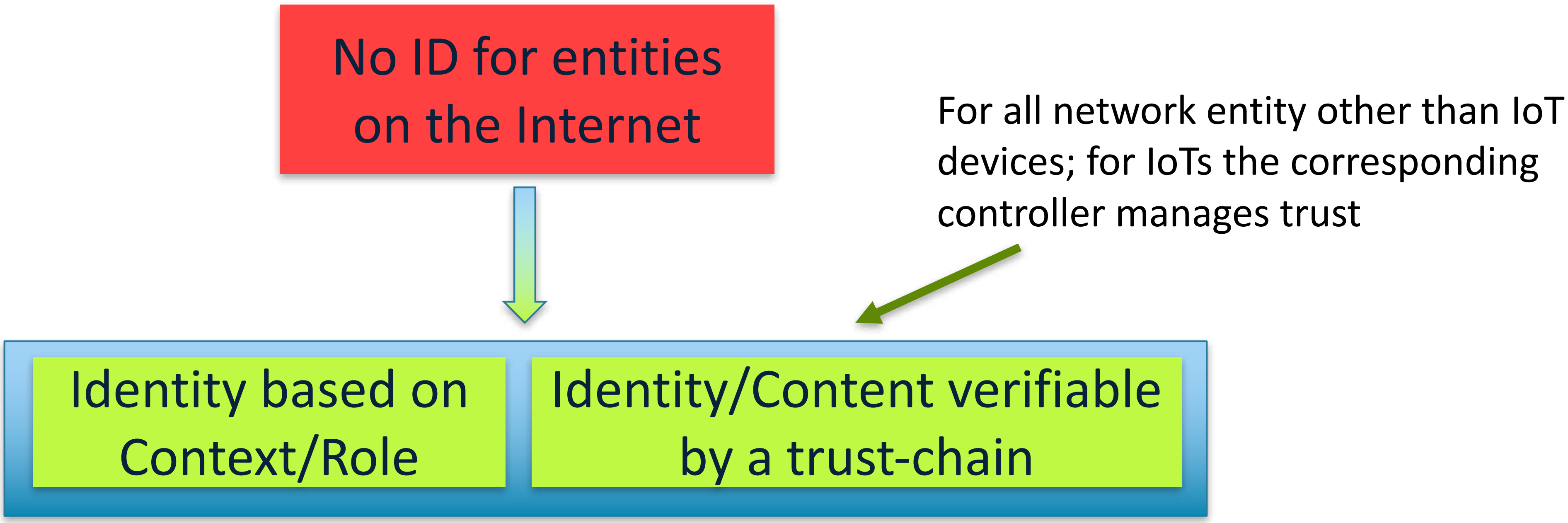
- NDN protocol stack
  - NFD: for network connectivity
- Routing configuration
  - Discovery of local hub & prefixes
  - Local data prefixes propagation
- Identity/Certificate
  - Sign Data with the certificate corresponded to identity
  - Data can be authenticated as it travels through the network

Identity Management



- Every application has corresponding identity (namespace) and certificate for this namespace
- Applications could manage sub-identities and their certificates (working in progress)

Schematized Trust at Scale



Specific Research Tasks:

- Trust rules *generalization* for the device universe;
- *Extension* to different trust settings (sp. Edge/IoT devices, AP, drone);
- *Automated* trust-level assignment for data based on reputation index for data sources;
- Conflating diverse data streams to increase information trust level.

Schematized Trust Illustration for on-campus scenario.

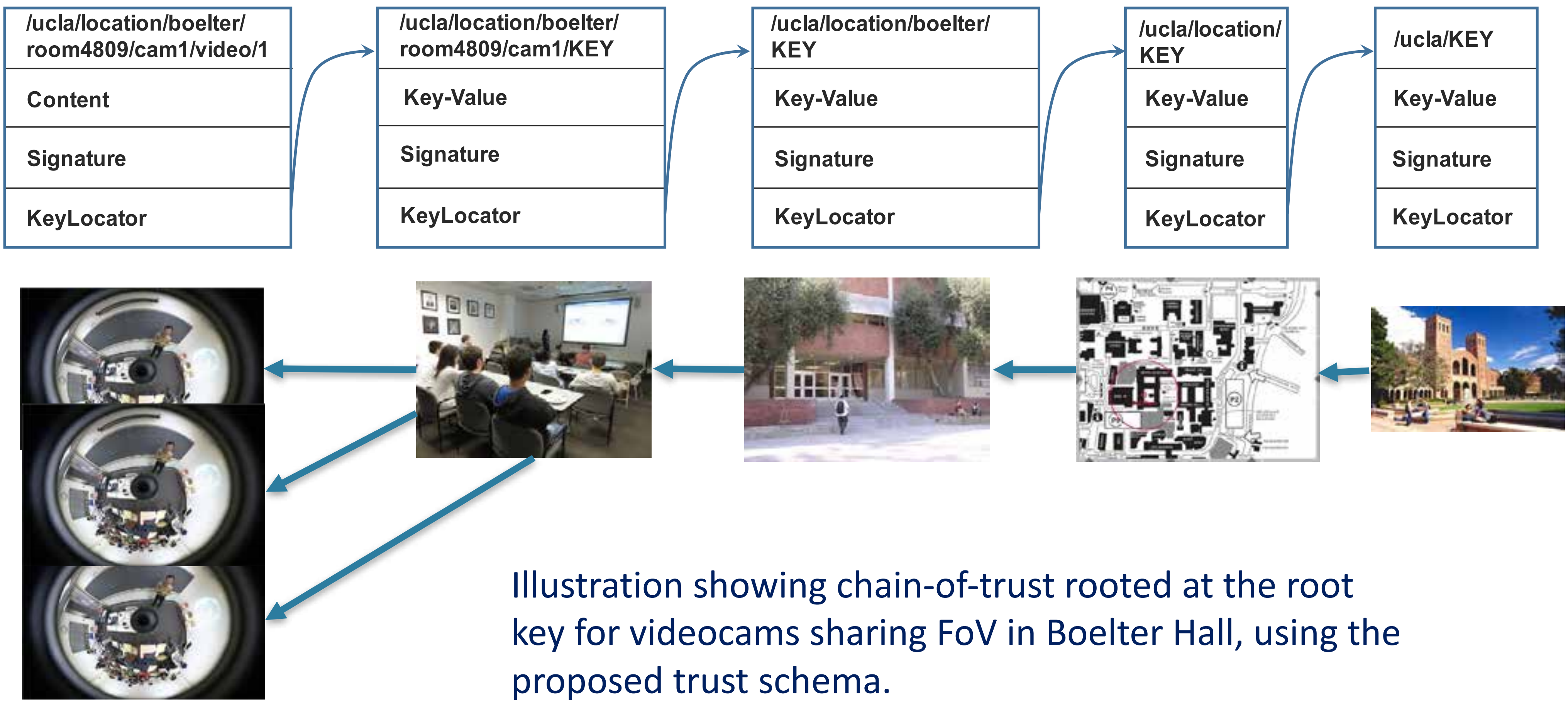


Illustration showing chain-of-trust rooted at the root key for videocams sharing FoV in Boelter Hall, using the proposed trust schema.

Named Data Security and Access Control at Scale

For all devices other than low-power "things".

Named Content: "/ucla/people /student/class/CS400"
Named Key: "/ucla/people/student/class/CS400/videocam/KEY"

For the low-power "things":

- hierarchical n/w
- mutually authenticated secure onboarding
- secure comms. with controller using symm. keys
- off-loading of computation to controller

Specific Research Tasks:

- exploring scalable AC using ABE, CP-ABE, broadcast enc.;
- extension of basic auth. model with secure on-boarding for IoT.
- **How to scale?**

Identity-mapping + trust-offloading: Capable devices.

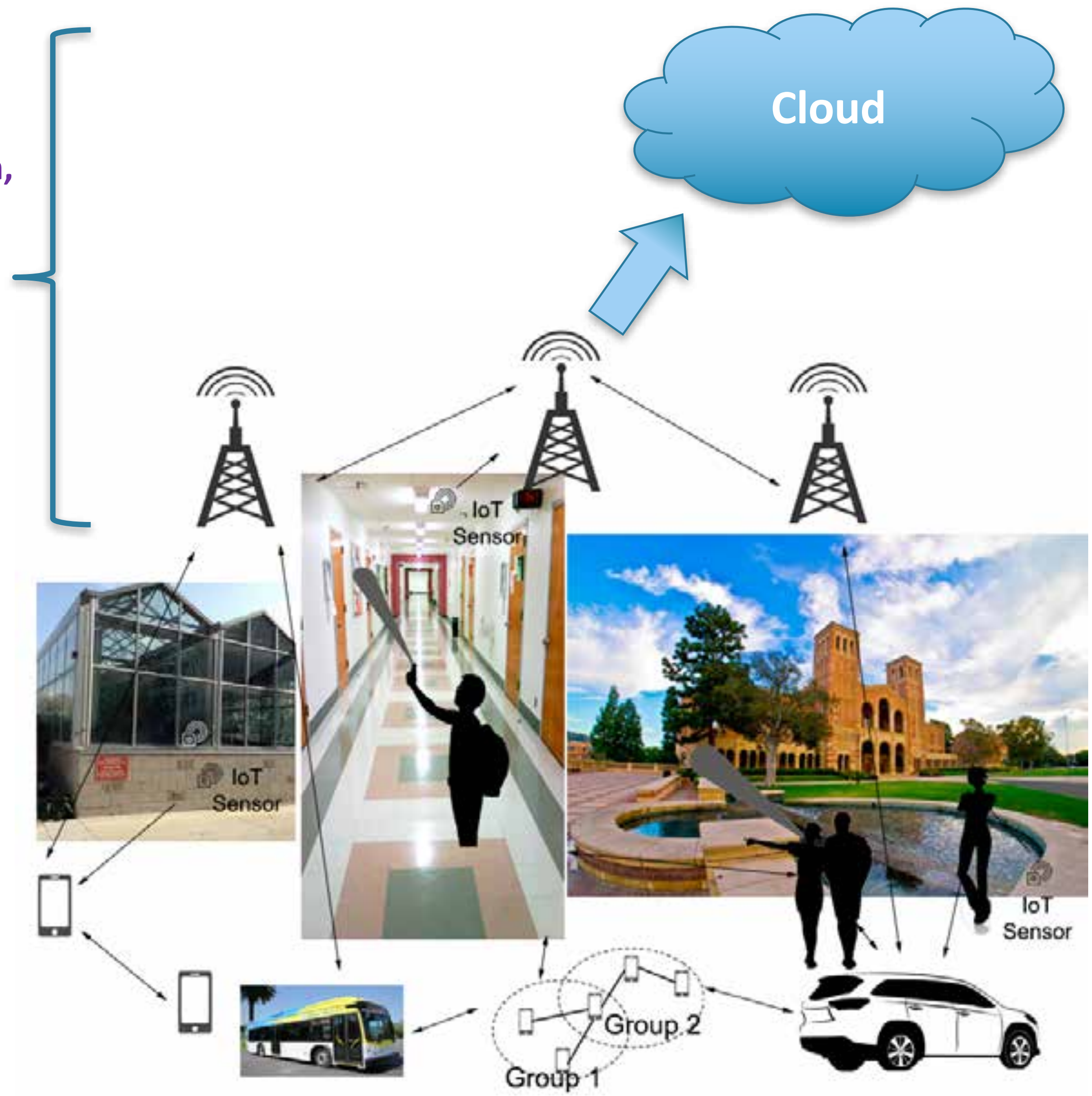
Up-to-the clouds

Data aggregation, processing, acceleration, coordination, anomaly detection, location certification, data publication

Foggy-bottom

PKI for bootstrapping and signatures

Dynamic session keys for content enc.



Reputation assessment

Access levels assignments and interactions

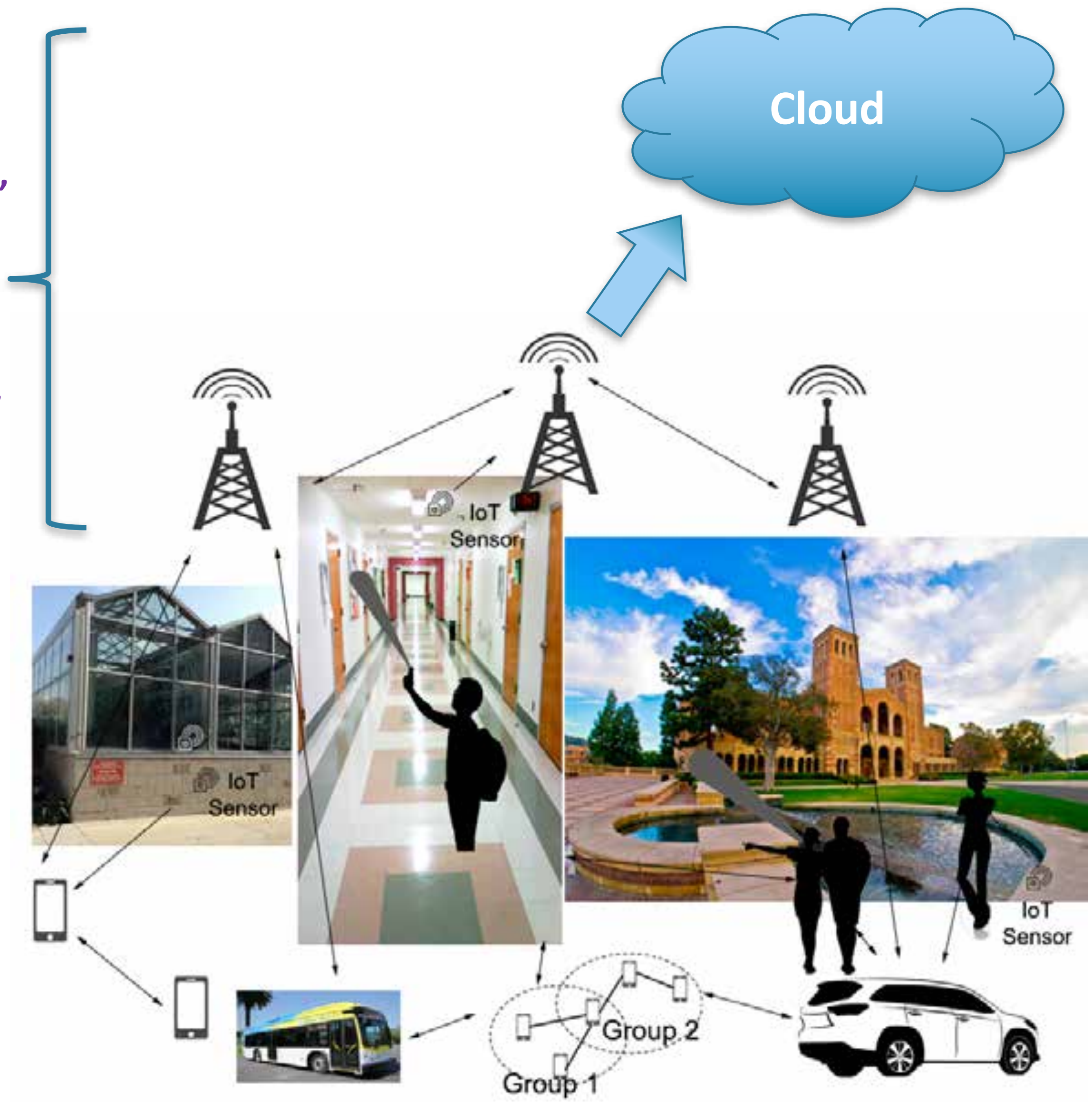
Identity-mapping + trust-offloading: IoT to Controller.

Up-to-the clouds

Data aggregation, processing, acceleration, coordination, anomaly detection, location certification, data publication; *namespace compaction; content re-encryption*

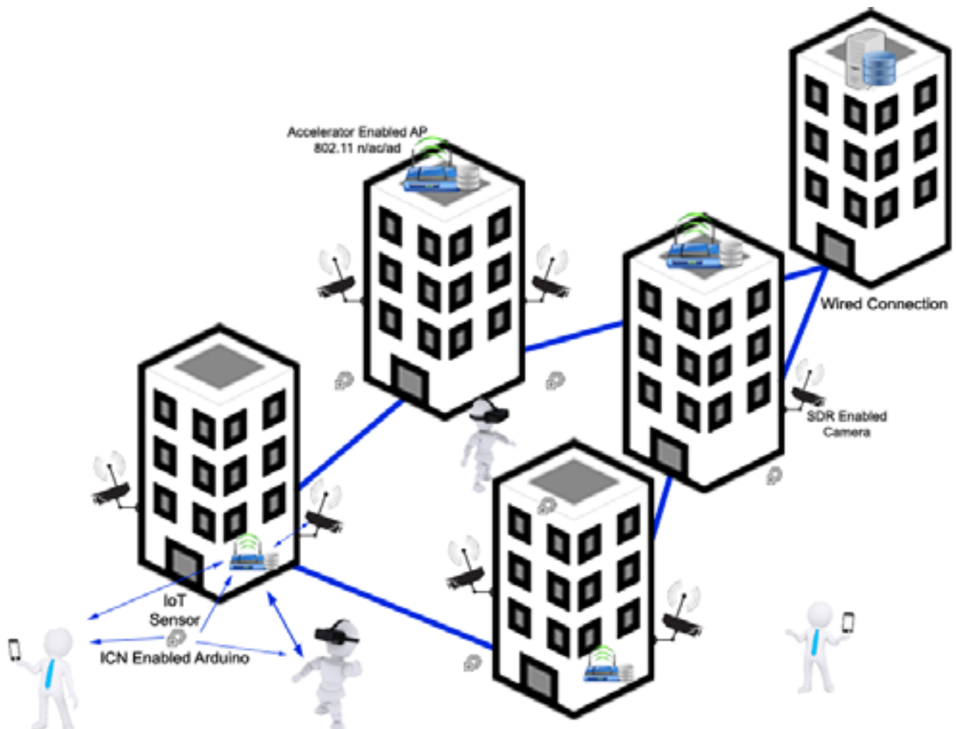
Foggy-bottom

Symmetric keys for enc./dec, message authentication



Transfer of reputation and access levels (Both data and operations)

Can we perform *secure, seamless* on-boarding and routing for devices?



Scalability, efficiency, synchronized multi-interface, multi-technology, configurability, security, …

Hierarchical topology, multi-level routing, identity-mapping, namespace management, …

User privacy in the many-to-many multi-source to multi-sink model

- Anonymity and accountability trade-off
  - Can we bridge the gap?
    - Conditional privacy with mutual authentication
- Challenges of multi-modal and large data volume generated by users
  - Diverse sources enable better analytics: Differential privacy?
- Challenges/opportunities in preserving privacy of devices/users
  - Scale, application diversity, technology diversity

Location-based Signature and Privacy at Scale

Granular, Location Based Identity	Efficient Signature Generation/Verification	Identity Privacy

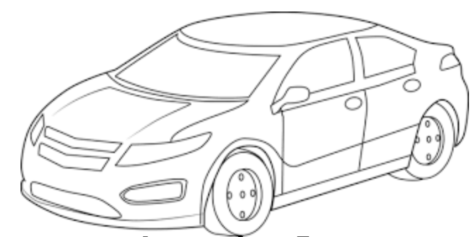
Specific Research Tasks:

- Efficient, private location-based namespace creation for all *producers (*including IoT devices);
- Signature generation/verification time efficiency techniques
  - (e.g., XORing packets' hashes for single verification) and
  - use of h/w acceleration;
- enhanced naming for efficient identity privacy for devices (including IoT devices) and users
  - pseudonyms, conditional privacy, anonymous mutual authentication

Where to use acceleration in security?

- Signature generation/verification and stronger content encryption:



- Faster encryption to reduce latency as needed, for content aggregation, query response, or post-processing data
  - Improving hardware implementations, e.g., Intel AES-NI
  - Implementing other symm. key algorithms (Speck, Simon, etc.*)
  - Named-functions for security and privacy-preserving computations.
- False Data Injection Mitigation
  - Wireless AP, aggregators, and controller
    - Correlating different data streams for in-network data/device validation

* D. Dinu, Y. L. Corre, D. Khovratovich, L. Perrin, J. Großschädl, and A. Biryukov. "Triathlon of Lightweight Block Ciphers for the Internet of Things." *IACR Cryptology ePrint Archive,* 2015, p.209. http://eprint.iacr.org/.

Things we have abstract ideas on.

- Use of schematized trust across the spectrum of "capable" devices
- Concept of name-based access control; where, how, when to use it?
- Location based signature and privacy and leveraging it
- Using AaaS for signatures, encryption, computations, etc.

Things we need to investigate.

- How to scale it up?

- Configurable security for the diverse devices in the ensemble?
  - Symm. keys, PKI, new ciphers, new reputation and access control mechanisms
- Security infrastructure working through disruptions?
- Security and privacy implications of data diversity and disruptions at scale?

Image Credits
http://raymondmatsuya.com/2016/becoming-an-automation-tester.php; https://blog.marketo.com/2013/03/accelerate-demand-using-rich-media.html

Thank you!