Inclusive Secure Information System for Community-Based ID Card Programs

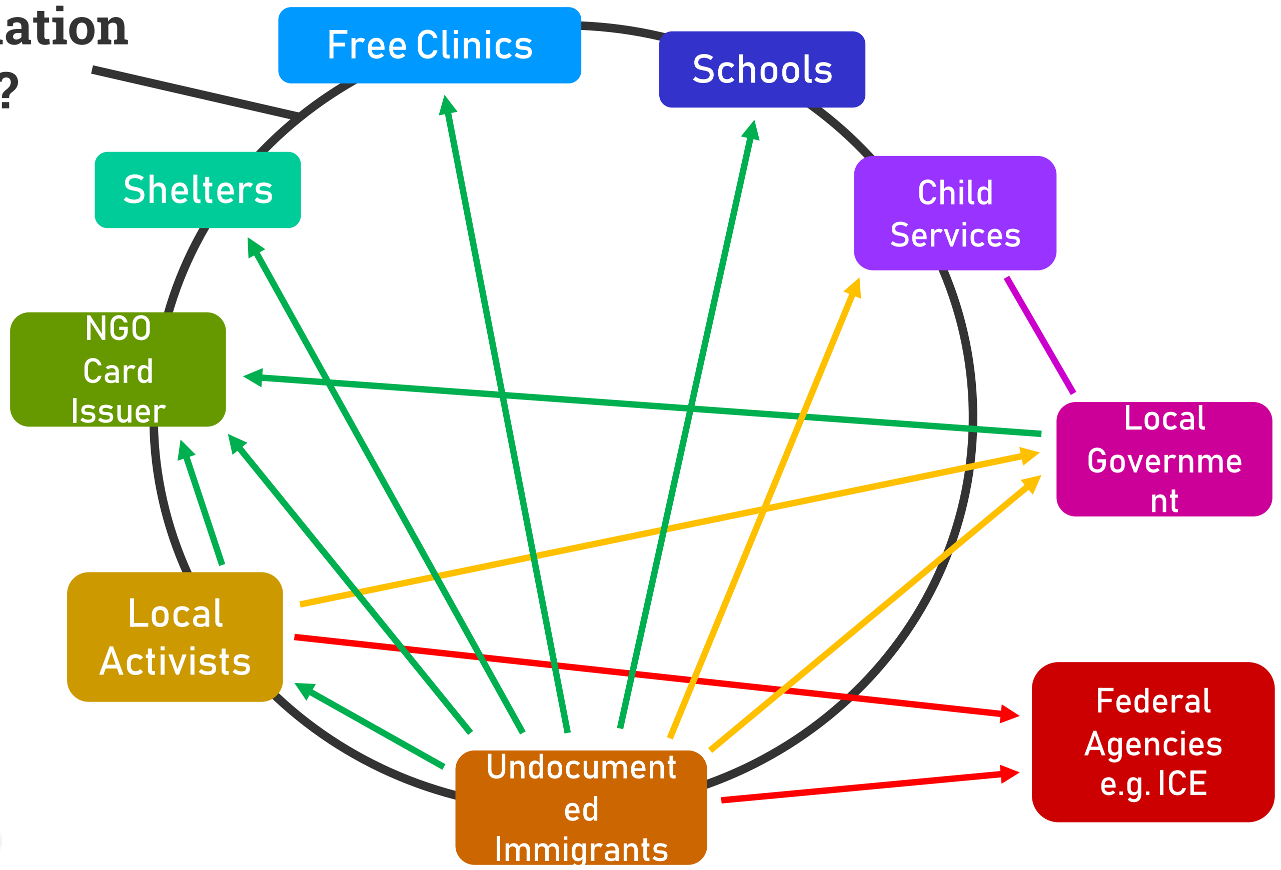
Ko (Natnatee) Dokmai,

Indiana University, Bloomington

Resident (Physical) ID Programs in Several Indiana Cities

*Disclaimer: Reductive model to facilitate discussion

How do we build a secure information ecosystem?



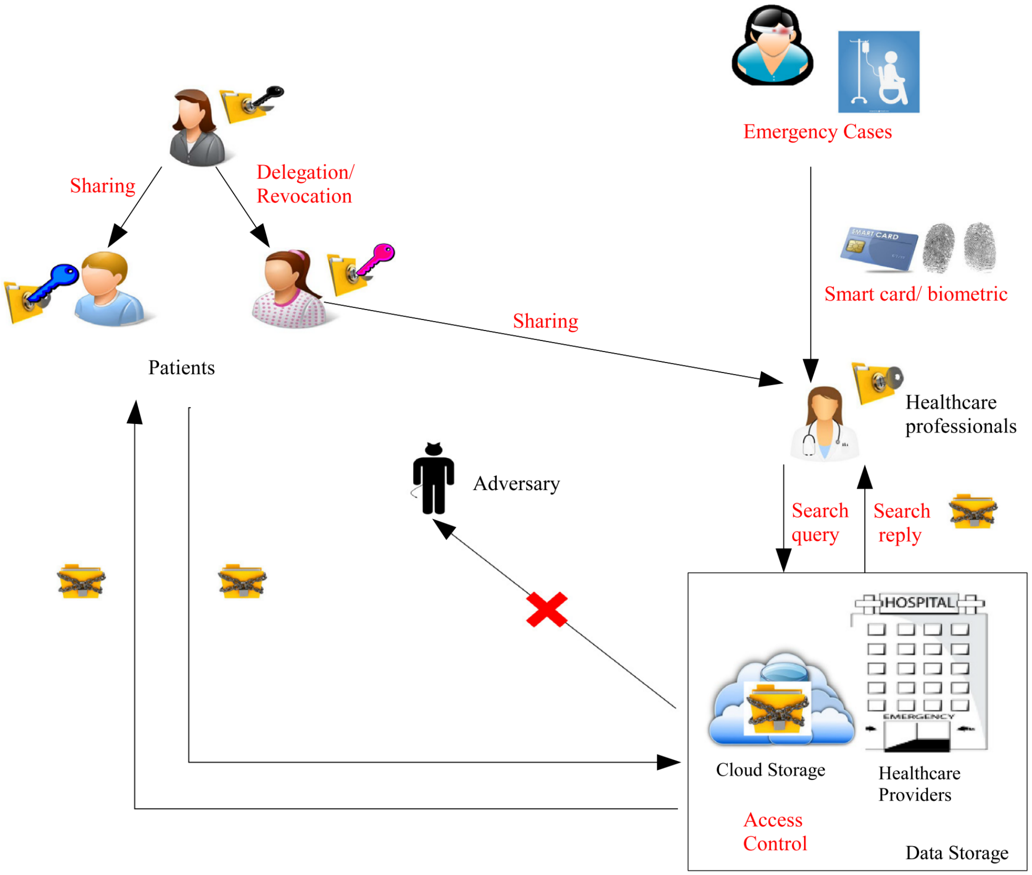
Challenges of Community-Oriented Secure Information System

- Complex security model to capture
- Design against strong adversaries
  - e.g. state-level adversaries
- Design in the lack of infrastructure
  - Network access
  - Computing devices

Addressed in this talk

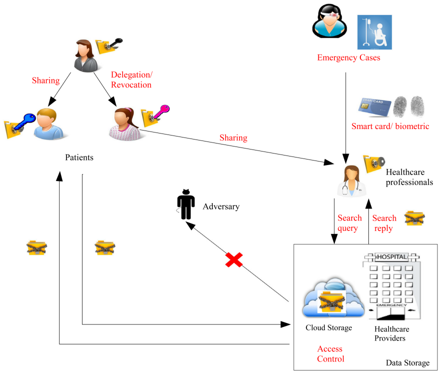
Approach: Community-oriented security design based on localized assumptions

From Electronic Health Records (EHR) to Community-Oriented Information System

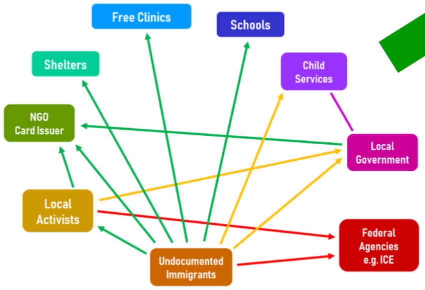


Electronic health services overview
(Yüksel, Küpçü and Özkasap, 2017)

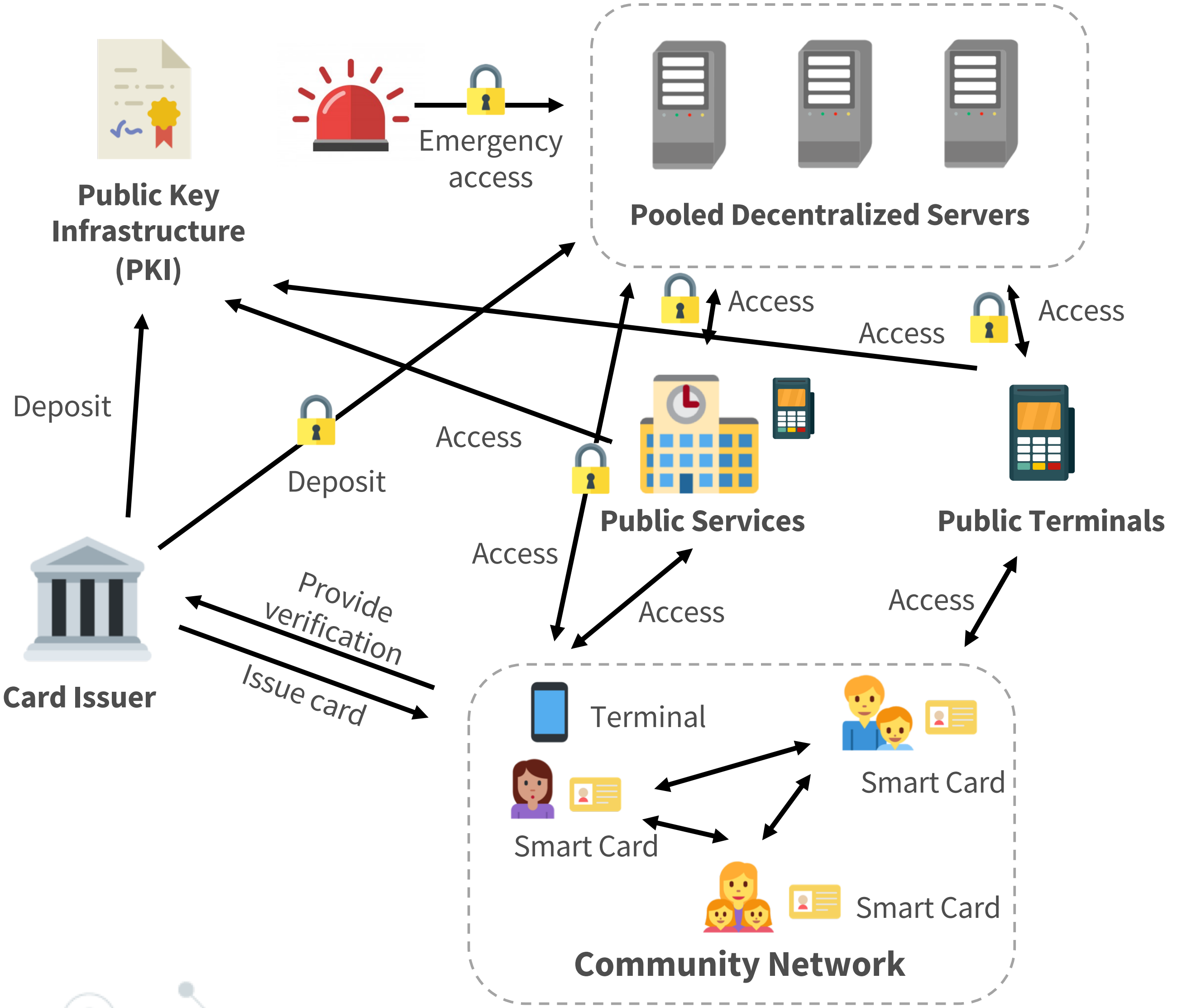
From Electronic Health Records (EHR) to Community-Oriented Information System



Base EHR Architecture



Trust Model



Key Techniques

Access Control

- Attribute-Based Encryption
- Threshold Encryption
- Multiple Encryption
- Zero-Knowledge Proof

Authentication Factors

- Smart Cards (Java Cards)
- PIN/Password
- Biometrics
- Trusted Parties

Anonymity

- Private Information Retrieval
- Mix-net

Recovery

- Proactive Secret Sharing

Emergency Access

- Trusted Parties Authentication

Revocation

- Unaddressed

Ongoing Work

- Assessment of smart card cryptography
- Practical private information retrieval
- Improve the model and architecture

Future Work

- Proof-of-concept implementation

References

- Yüksel, B., Küpçü, A. and Özkasap, Ö. (2017). Research issues for privacy and security of electronic health services. *Future Generation Computer Systems*, 68, pp.1-13.