Microsoft Research
FacultySummit

Encryption as Access Control for Cloud Computing

Carl A. Gunter
Professor
University of Illinois at Urbana-Champaign

FUTURE WORLD
2011 2031

Health Information Technology Demands

- Health Information Technology (HIT) for healthcare providers was typically an in-house operation.
- Key demands are changing this:
  - Supporting Electronic Health Records (EHRs) even at small providers
  - Providing EHR data to patients in Personal Health Records (PHRs)
  - Sharing EHR data with other providers in Health Information Exchanges (HIEs)
  - Sharing EHR data for public health and medical research
  - New remote monitoring capabilities: devices and telemedicine

HIT Meets Cloud Computing

- Providers are now reflecting on the prospects for using cloud computing to address these demands
- Examples
  - Hosted EHRs
  - PHR providers (tethered or independent)
  - Hosted HIE systems (examples: Indiana and Memphis)
  - Hosted research systems (example: Mayo Clinic cloud)
  - Assisted Living Service Providers (ALSPs) and data collection services provided by device vendors.

Is Cloud Computing Secure Enough for These Applications?

- Inquiring providers, patients, and others want to know.
- Test question: who accepts liability for losses?
  - Data breaches are now common and serious with non-trivial penalties and severe adverse publicity.
  - Who is in the best position to protect the data appropriately, the parties who create and use it or the ones holding it?

Using Encryption

- Encryption provides a strategy to mitigate risks to hosted data.
- Simple examples:
  - Research data is kept in a cloud but is de-identified to mitigate risk.
  - Backup data is kept by a backup server but is encrypted with a key held by the provider.

Encryption as Access Control (EAC)

- Taking this idea further: what if access control by the provider could enforce the protections expected of the hosting system?
- Access controls can still be expected from the host, but refined or backed up by encryption by the data provider.
- Concept: Encryption as Access Control
  - Also known as "cryptographic access control" or "encryption-based access control"

Pros and Cons of EAC

Pros

- Puts protection capabilities into the hands of the parties who create and use the data
- Data is “self protecting”
- Provides protection against the hosting service

Cons

- Limits the ability of the host to provide services (viz. search)
- Key management is required
- Efficiency can be a concern
- “Traffic” analysis is a risk

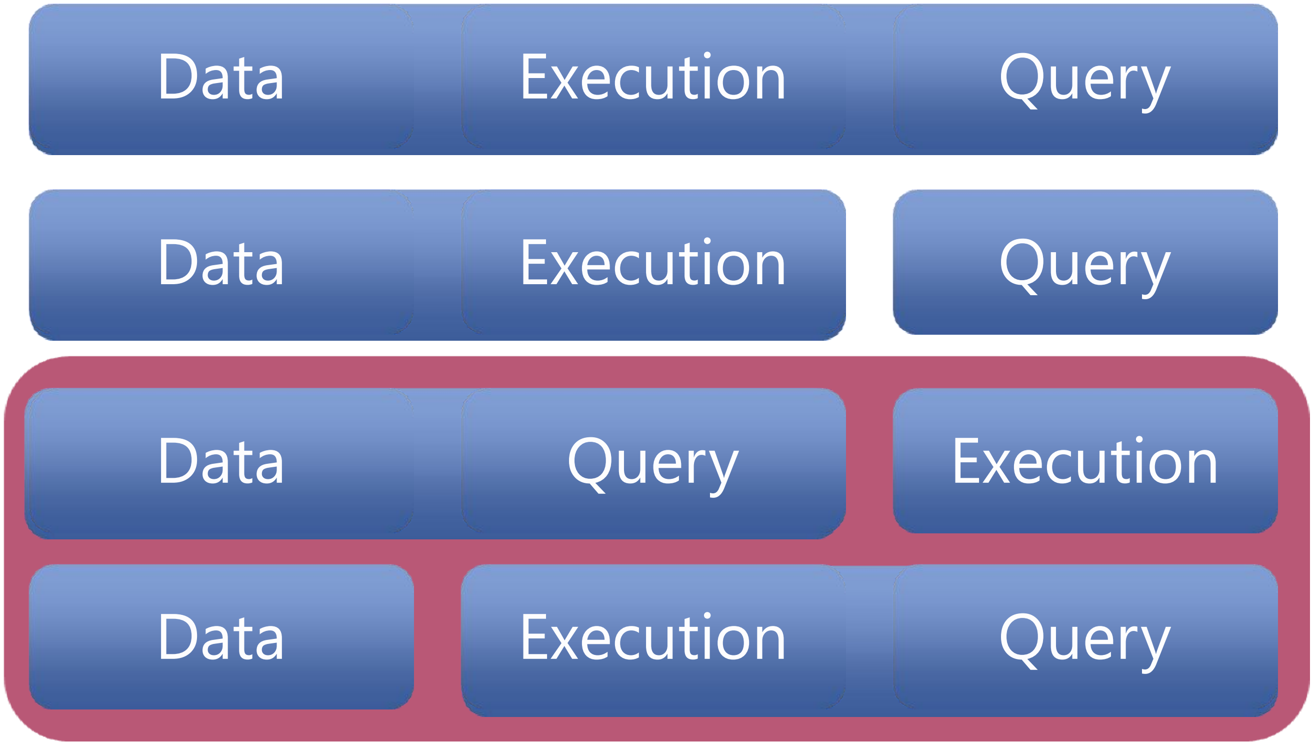
Architectural Perspective on Trust Domains

Single User DBMS

Client / Server

Database as a service
(aka Cloud Service)

Data Publishing
(aka EAC)

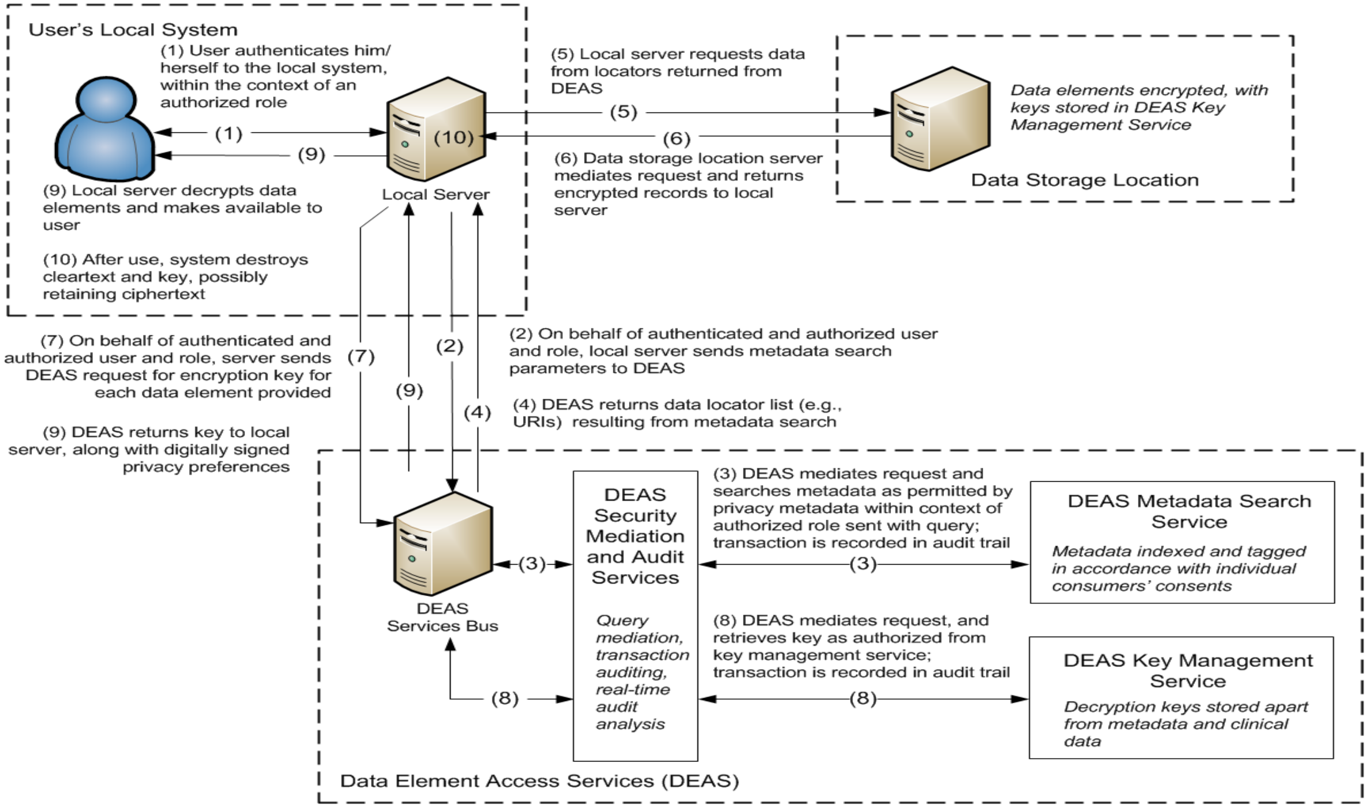


Case Study: Nationwide HIE Architecture from the PCAST HIT Report

- Recent report from the Presidential Committee of Advisors on Science and Technology recommends the use of EAC as part of a large-scale HIE system.
- Basic use case: provider X needs radiology images for patient Y when Y seeks treatment from X. Query from X to HIE system retrieves all images X and Y consider to be appropriate.

PCAST HIT Architecture

PCAST HIT EAC



Proposed Metadata Wrapper

Metadata Element	CDA R2 Example
Envelope	<?xml version="1.0" encoding="UTF-8"?> <ClinicalDocument xmlns="urn:hl7-org:v3">
Provenance - TDE ID	<id extension="http://stelsewhere.com/id/12345" assigningAuthority="St. Elsewhere Hospital"/>
Privacy - Content Data Type	<code code="34788-0" displayName="Psychiatric Consult note" codeSystemName="LOINC"/>
Provenance - Timestamp	<effectiveTime value="20011217093047"/>
Privacy - Content Sensitivity	<confidentialityCode code="PSY"/>
Boilerplate	<recordTarget> <patientRole>
Patient ID - ID	<id extension="1234567" root="http://www.nh.gov/safety/divisions/dmv/"/>
Patient ID - Address	<addr use="HP"> <streetAddressLine>1234 Main St. Apt 3</streetAddressLine> <city>Bedford</city> <state>MA</state> <postalCode>01730</postalCode> </addr>

Metadata Element	CDA R2 Example
Patient ID - Name	<patient> <name> <prefix qualifier="AC">Dr.</prefix> <given> John</given> <given>William</given> <family>Smith</family> <displayName>Dr. John William Smith</displayName> </name>
Patient ID - DOB	<birthTime value="19600427"/>
Boilerplate	</patient> </patientRole> </recordTarget>
Boilerplate	<author> <assignedAuthor>
Provenance - Actor	<assignedPerson> <providerDirectoryEntry href="http://providerdirectory.org/1234"/> <name> <family>Smith</family> <given>John</given> <prefix>Dr.</prefix> </name> </assignedPerson>
Provenance - Affiliation	<representedOrganization> <id extension="http://stelsewhere.com/" assigningAuthority="St. Elsewhere Hospital"/> <name>St. Elsewhere Hospital</name> <telecom use="1-800-555-1234"/> </representedOrganization>
Boilerplate	</assignedAuthor> </author>
Envelope	</ClinicalDocument>

Challenges

- Has this sort of architecture been tried at this scale?
- Who runs the DEAS?
- There will be a lot of sensitive information in just the headers; how many principals will have access to this data? Would encrypted search help?
- How granular can or should the records be? Data segmentation is a hard problem.

Strategic Healthcare Advanced Research Projects for Security

SHARPS

Strategic Healthcare Advanced Research Projects **(SHARP)** is sponsored by the Office of the National Coordinator of the United States Department of Health and Human Services.

Began in April 2010 and lasts 4 years

SHARPS Rationale

- Cyber security and privacy (S&P) risks are a significant barrier to the deployment and meaningful use of health information technology.
- Many key challenges in these areas can be addressed with emerging and new technologies in S&P.
- SHARPS teams computer scientists who specialize in S&P with healthcare specialists interested in S&P for HIT. The aim is to produce new levels of communication and tech transfer.

www.sharps.org

SHARPS Environments

- **EHR** – Electronic Health Records, managing patient records within an enterprise
- **HIE** – Health Information Exchange, sharing records between enterprises or between an enterprise and a patient in the form of a Personal Health Record
- **TEL** – Telemedicine, monitoring remotely, communicating with multimedia, and controlling implanted medical devices

SHARP Research Areas

- Security and Privacy **(SHARPS)**
- Patient-Centered Cognitive Support
- Health Applications and Networking Platforms
- Secondary Use of Health Records

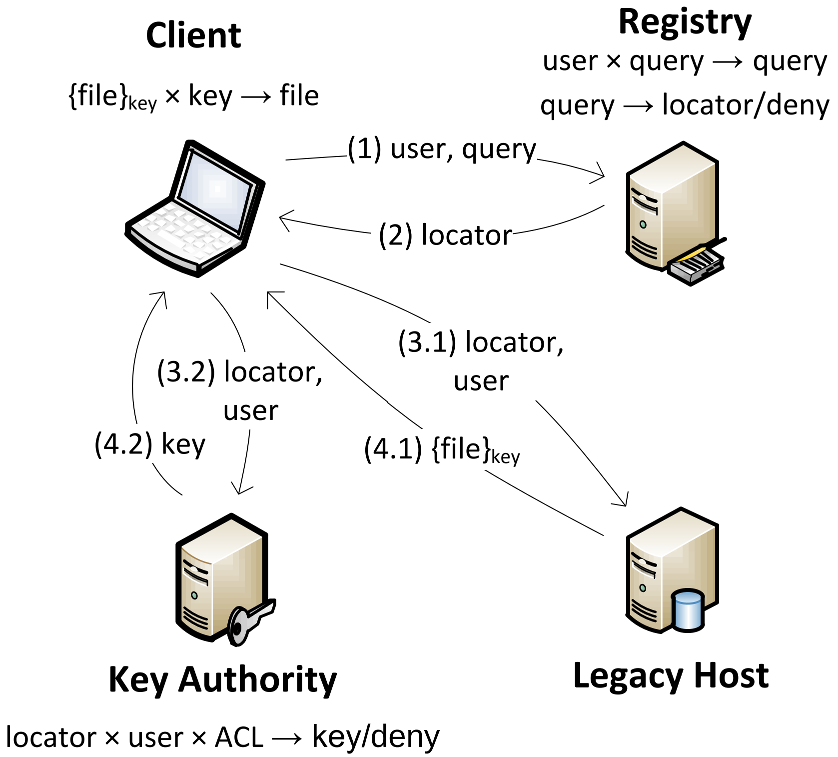
http://HealthIT.HHS.gov/sharp

SHARPS Participating Institutions

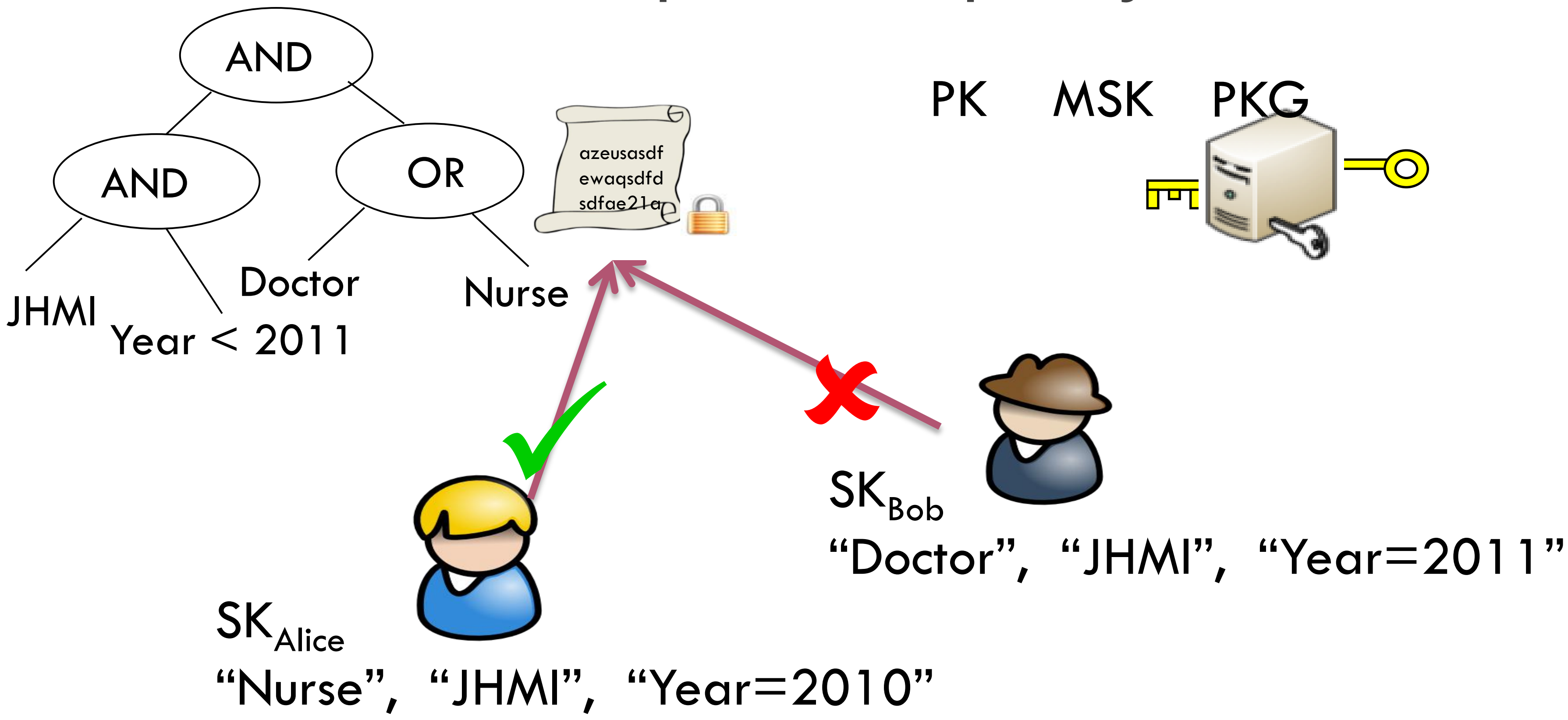
- University of Illinois at Urbana-Champaign
- Carnegie Mellon University
- Dartmouth College
- Harvard University and Beth Israel Deaconess Medical Center
- Johns Hopkins University and Children's Medical and Surgical Center
- New York University
- Northwestern University and Memorial Hospital
- Stanford University
- University of California, Berkeley
- University of Massachusetts Amherst
- University of Washington
- Vanderbilt University

EAC Subversion

- Proof of concept prototype to explore EAC as a way to add advanced access control to a legacy database as a service
- Modest changes to SVN client to manage encryption
- No changes to server



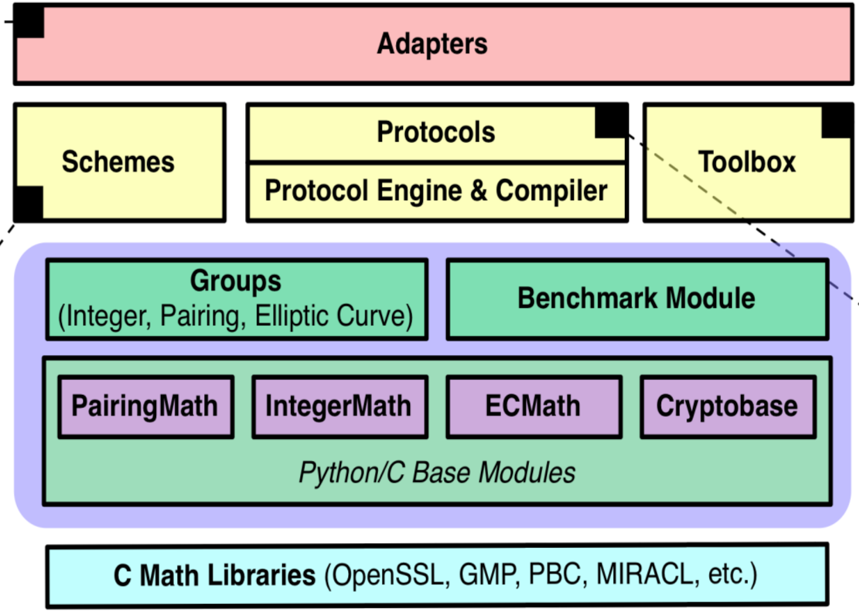
ABE: Ciphertext-policy



Charm

ADAPTERS Thin wrappers that alter the input/output or security properties of a scheme. This promotes code re-use by removing incompatibilities between implementations.

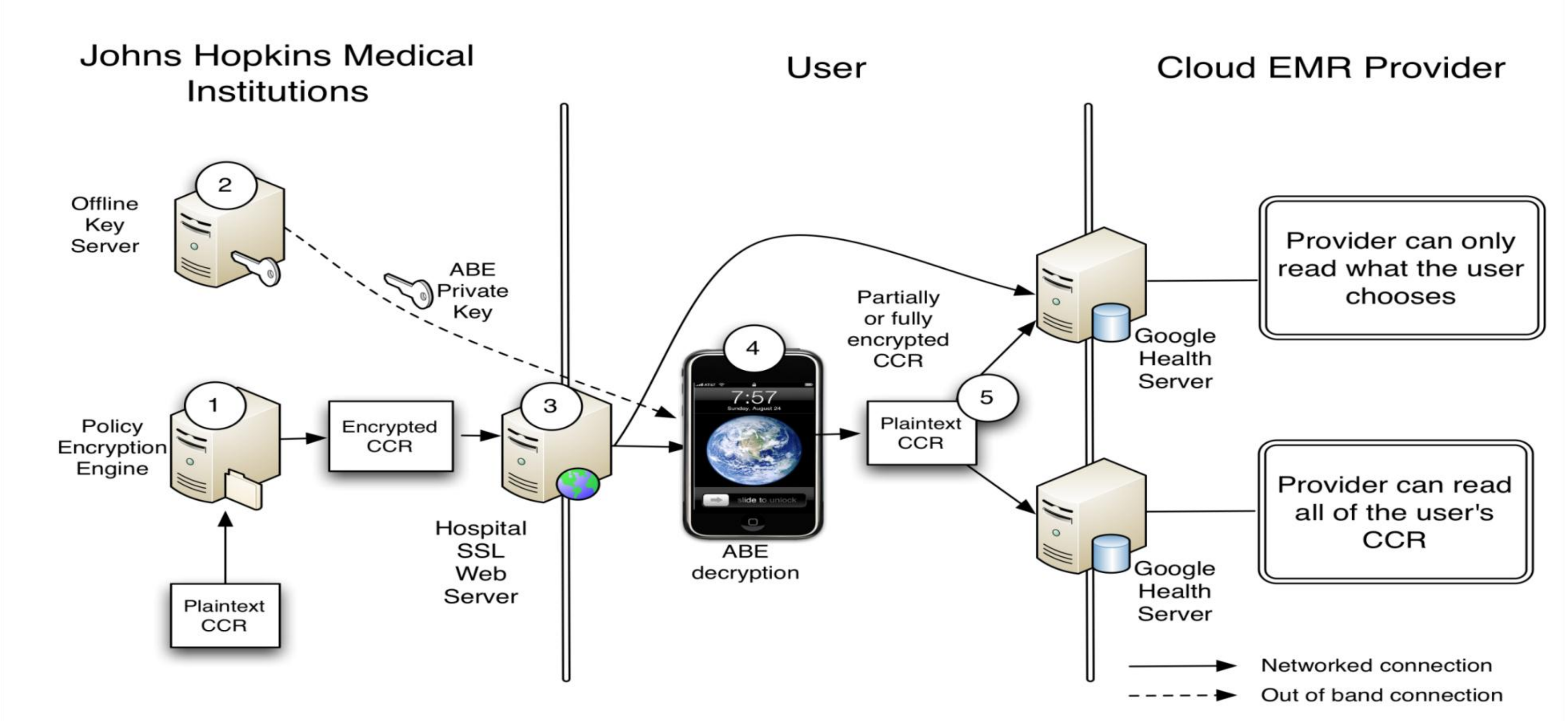
SCHEMES A library of implemented cryptosystems, accessed via standard scheme APIs.



TOOLBOX Extensible library of common routines, including secret sharing, X.509 certificate handling, parameter generation, policy parsing, and hash functions.

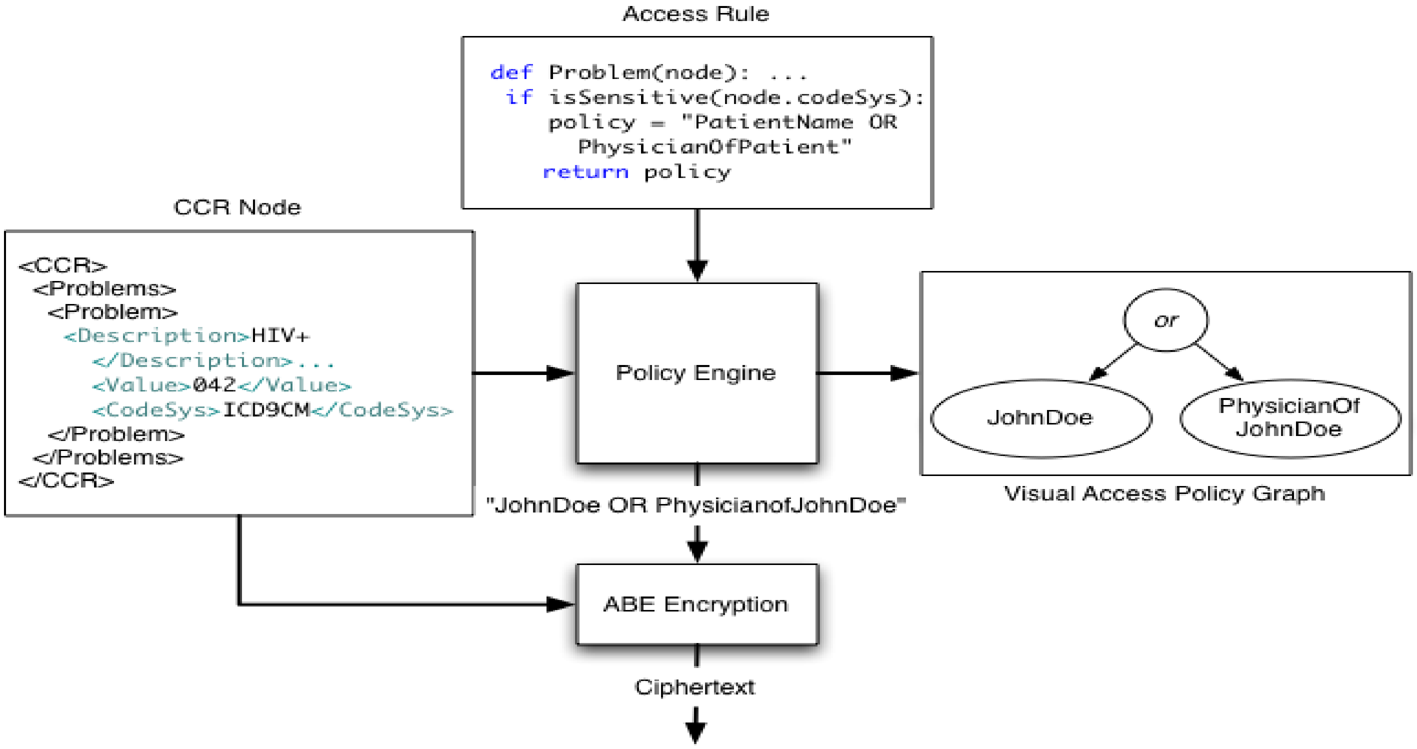
PROTOCOLS Infrastructure to support the development of interactive protocols via a dedicated protocol engine. A proof compiler provides support for protocols that use ZK proofs.

Charmed PHRs: Architecture

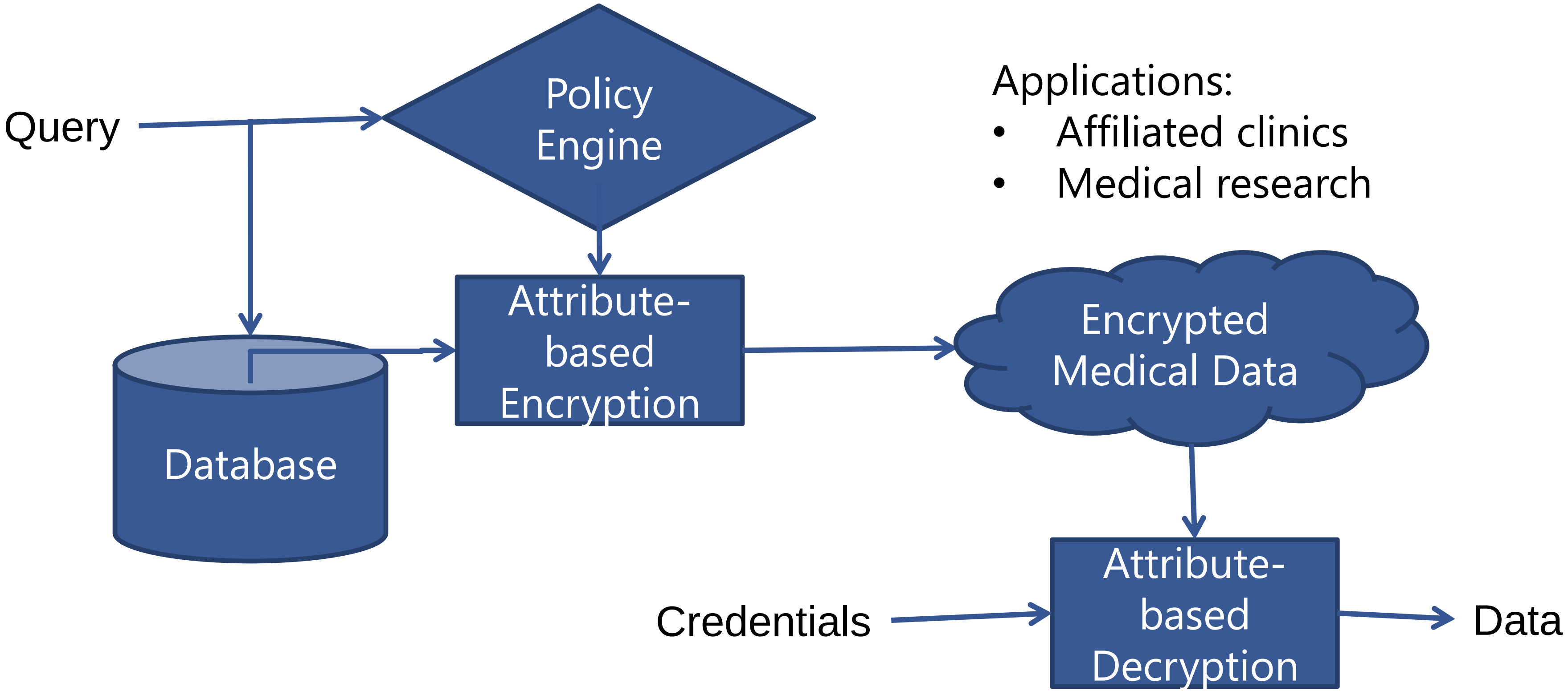


Akinyele Lehmann Green Pagano Peterson Rubin

Charmed PHRs: Policy Engine



ABE EAC for Medical Data in Clouds



Applications:

- Affiliated clinics
- Medical research

Lam Mitchell Scedrov Sundaram Frank Wang

Extracting ABE data policy

- HIPAA, Hospital policy
  - Mapping : Action → {allow, deny}
  - Action: ⟨to, from, about, type, purpose, consents, beliefs⟩
- Action characterized by
  - Attributes of data: from, about, type, consents
  - Attributes of recipient: to, purpose, belief

- Data policy
  - Data with attributes: from, about, type, consents
  - Has associated access policy

    {⟨to, purpose, beliefs⟩ |

    Policy(⟨to, from, about, type, purpose, consents, beliefs⟩) = Allow}

Secure HIE Prototype

Related Work (SHARPS)

- *PCAST Workgroup Letter to the National Coordinator,* Paul Egerman (Chair), Bill Stead (Vice Chair) and the PCAST Workgroup Members, ONC Policy Committee, April 2011.
- *Encryption as Access Control in Legacy Hosted Systems*, Kyle Blocher, Igor Svecs, and Carl A. Gunter.
- *Self-Protecting Electronic Medical Records Using Attribute-Based Encryption*, Joseph A. Akinyele, Christoph U. Lehmann, Matthew D. Green, Matthew W. Pagano, Zachary N. J. Peterson, and Aviel D. Rubin.
- *Declarative Privacy Policy: Finite Models and Attribute-Based Encryption*, Peifung E. Lam, John C. Mitchell, Andre Scedrov, Sharada Sundaram, and Frank Wang.

Related Work (Selected)

- *Controlling Access to Published Data Using Cryptography,* Gerome Miklau and Dan Suciu, VLDB 03.
- *Report to the President Realizing the Full Potential of Health Information Technology to Improve Healthcare for Americans: The Path Forward*, Executive Office of the President President's Council of Advisors on Science and Technology. The PCAST Report 10.
- *Patient Controlled Encryption: Ensuring Privacy of Electronic Medical Records,* Josh Benaloh, Melissa Chase, Eric Horvitz, and Kristin Lauter. CCSW 09.
- Over-Encryption: Management of Access Control Evolution on Outsourced Data, Sabrina De Capitania di Vimercati et. al. VLDB 07.

Conclusions

- Trends in health information technology are spurring interest in cloud computing.
- Security and privacy protections in clouds are a key concerns for providers and patients.
- Encryption as access control offers a practical strategy for these mitigating risks.
- There are rich opportunities for applications of existing and new ideas in architectures and cryptography.