

MedVault: Ensuring Security and Privacy for Electronic Medical Records

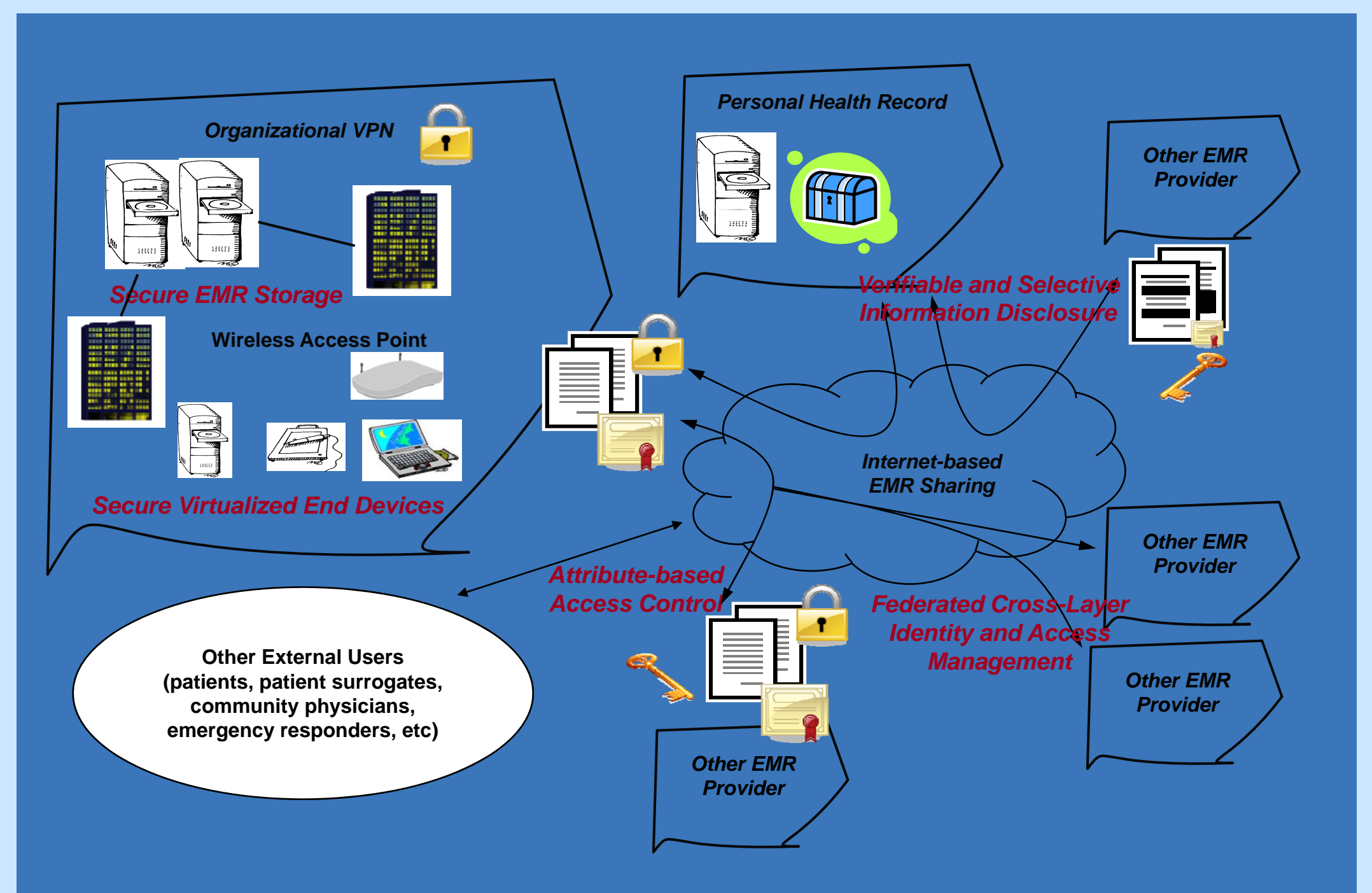
Douglas Blough, Mustaque Ahamad, Ling Liu, Praveen Chopra
Georgia Institute of Technology, Children's Healthcare of Atlanta

Goal

The advent of large-scale sharing of medical information can be compared to the development of the Internet in two ways: it will enable major leaps in efficiency and quality of patient care, and it will create numerous opportunities for malicious parties to abuse the information. The goal of this project is to develop new techniques for the storage, maintenance, and control of sensitive data that permit open sharing among a wide variety of legitimate users while protecting the data against unauthorized use and disclosure.

Challenges

- flexible access control mechanisms and policies in a federated environment
- integration of privacy and access control mechanisms with secure storage techniques
- protection of data everywhere, including on end devices that are the most vulnerable points
- integration of technological solutions with the overall health system and medical processes.



New approach

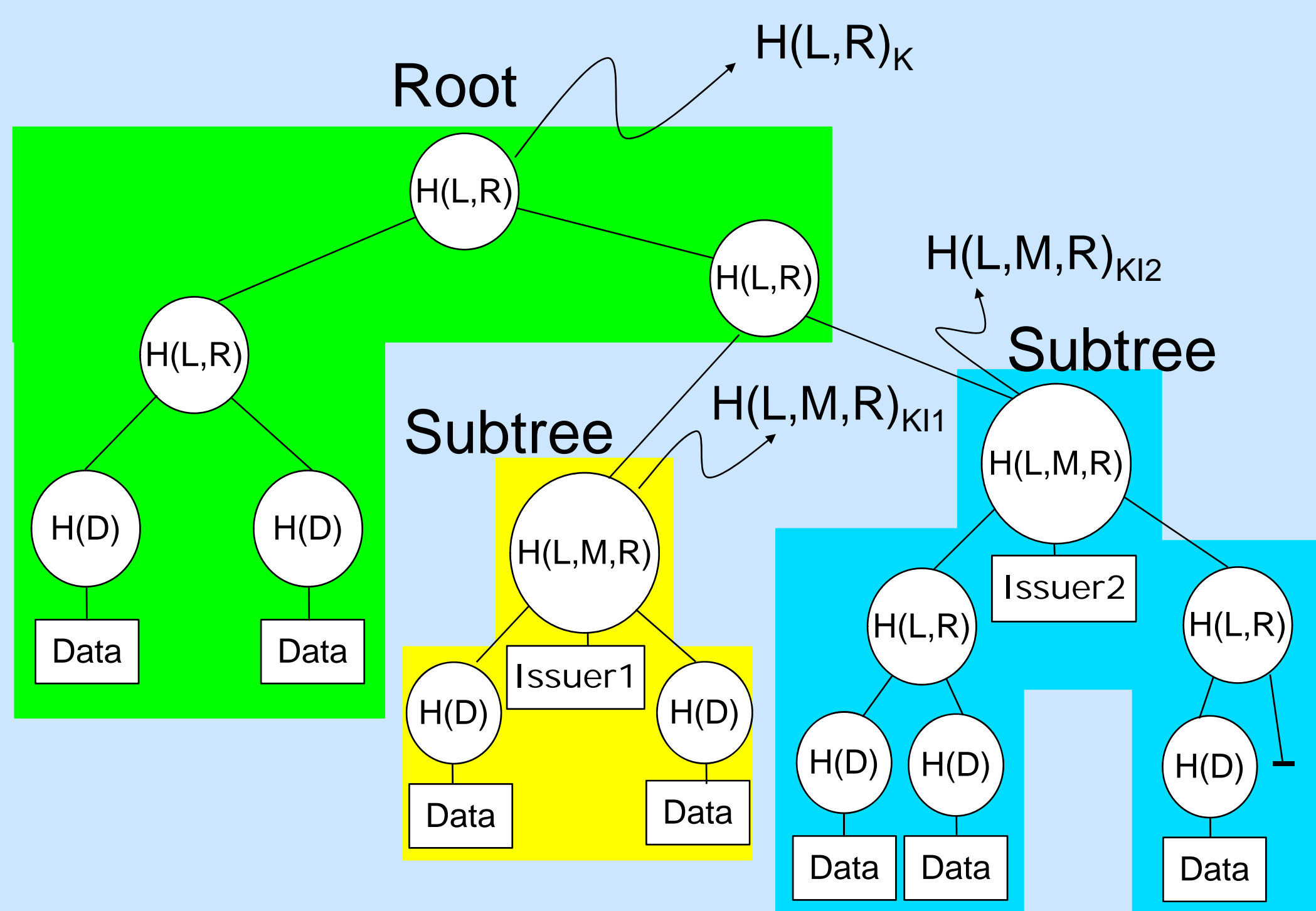
- Cross-layer identity and access management
- Distributed secret-shared caching
- New redactable signature techniques

Approach and Impact

- Ability to authorize and control operations in federated environments
- Strong confidentiality with improved performance in widely distributed environments with mobile users
- Verifiable personal health records with selective disclosure

Research Impact

Research Example: Redactable Signatures for Personal Health Records



- allow patients to store their own copy of verifiable medical data from health care providers and selectively disclose it to other entities
- Merkle-hash-tree-based redactable signatures provide the basic mechanism, extended to allow multiple authorities and data dependences
- providers supply signed hash tree to personal health record service
- patients can selectively provide verifiable health information to other entities, possibly with restrictions on data combinations
- entities can detect if information has been tampered with and can verify source signature
- patient can annotate but not modify information