Microsoft Research

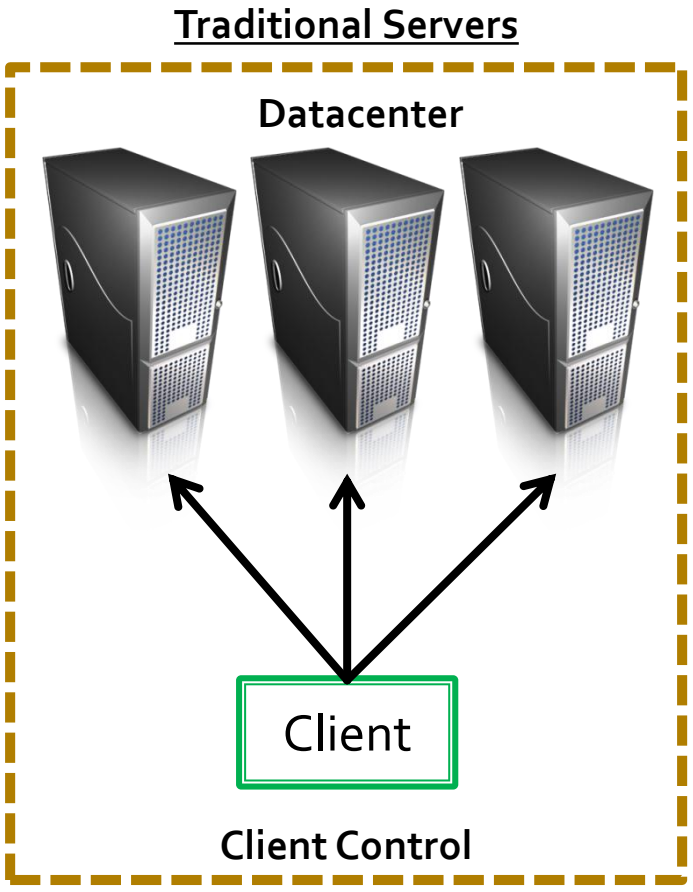
FPGAs for Trusted Cloud Computing

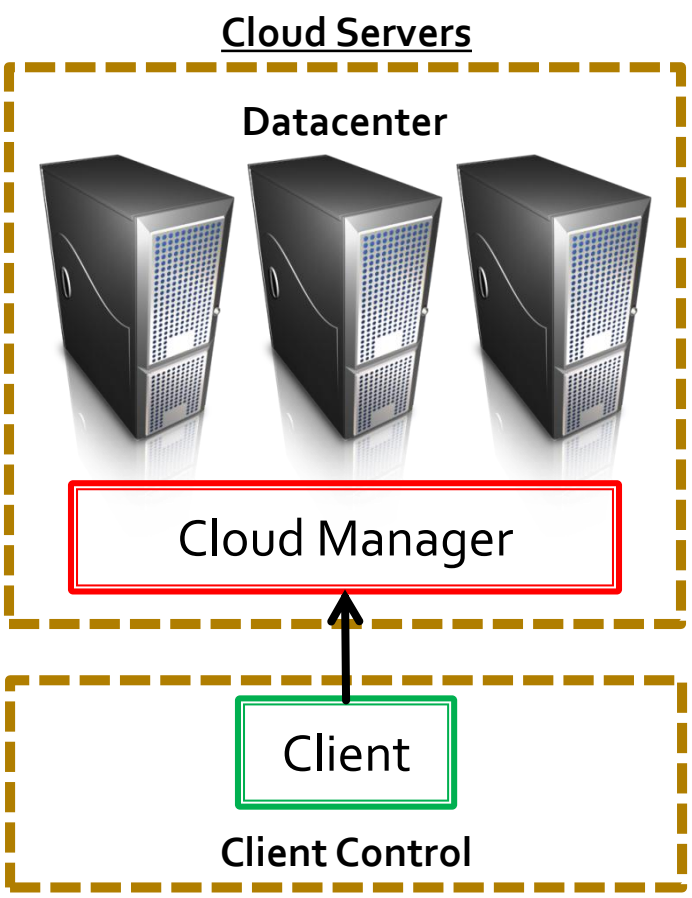
Ken Eguro
Embedded and Reconfigurable Computing

Ramarathnam Venkatesan
Cryptography, Security and Applied Mathematics

FPL 2012 – Oslo, Norway
August 29th

Cloud Computing

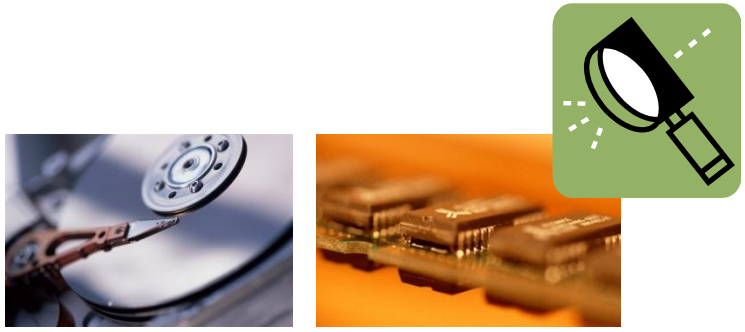




Cloud Security Issues

- Existing cloud systems cannot offer strong security guarantees
  - Cloud administrator access ➔ liability
  - Availability & co-tenancy ➔ malware & side-channel attacks

Cloud administrators have full access!



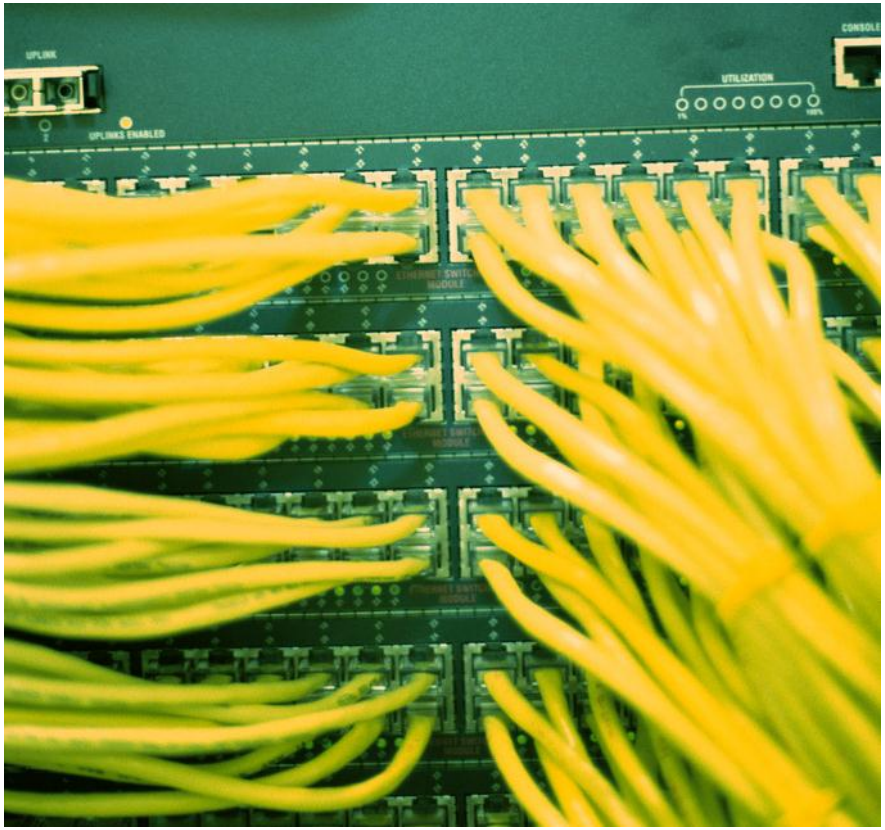
Cloud Security Issues

- Existing cloud systems cannot offer strong security guarantees
  - Cloud administrator access ➔ liability
  - Availability & co-tenancy ➔ malware & side-channel attacks

Cloud is open to everyone!

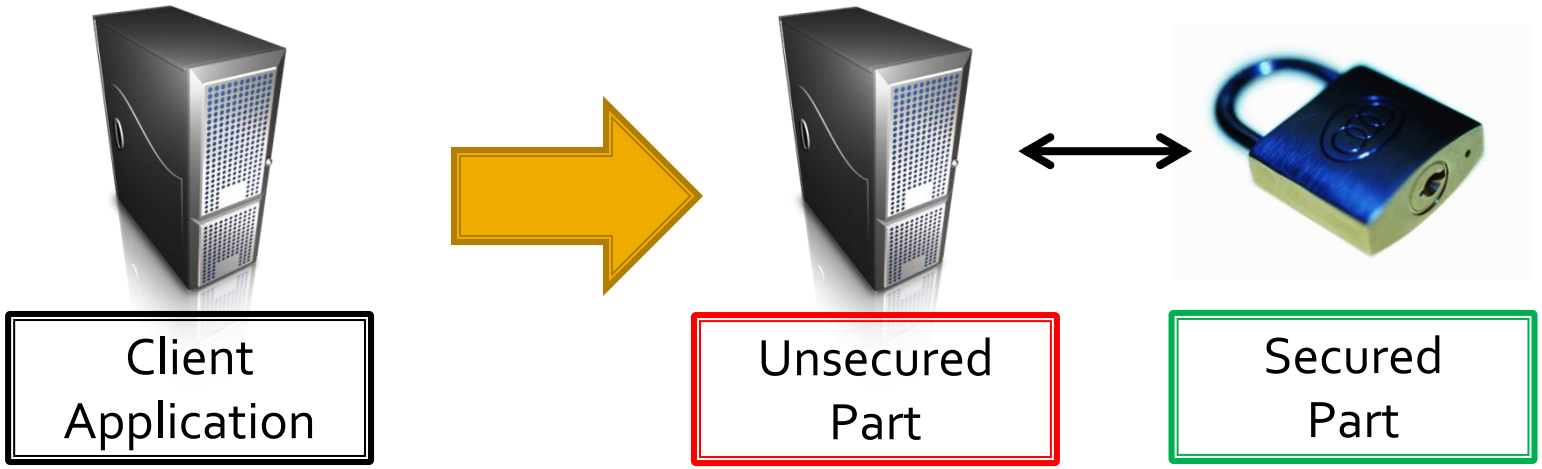
Service-Level Agreements

- Network bandwidth/ latency
- CPU time
- Storage allotment/ latency
- Minimum uptime
- ~~Security~~



Observation: Security Imbalance

- 1% to 10% of information/transactions deal with sensitive data
- Isolate only sensitive computations on trusted compute nodes



Trusted Compute Node

- Independent administration
  - Management != full access
  - Cloud operator is not part of "root of trust"
- Physically secure
- High performance
- Generality
- Flexibility

Trusted Compute Node

- Independent administration
- Physically secure
  - Store keys
  - Decrypt & authenticate binaries and data
  - Execute application exactly as prescribed
- High performance
- Generality
- Flexibility

Trusted Compute Node

- Independent administration
- Physically secure
- High performance
- Generality
- Flexibility

Process of Elimination

- Requirements
  - Independent administration √
  - Physically secure X
  - High performance √
  - Generality √
  - Flexibility √
- Platform Options
  - Commodity servers
  - Local/cloud hybrids
  - High security commodity servers
  - Secure co-processors
  - Homomorphic crypto
  - Dedicated hardware
    - HSMs
    - FPGAs

Process of Elimination

- Requirements
  - Independent administration √
  - Physically secure √
  - High performance X
  - Generality X
  - Flexibility X
- Platform Options
  - ~~Commodity servers~~
  - Local/cloud hybrids
  - High security commodity servers
  - Secure co-processors
  - Homomorphic crypto
  - Dedicated hardware
    - HSMs
    - FPGAs

Process of Elimination

- Requirements
  - Independent administration √
  - Physically secure √
  - High performance X
  - Generality X
  - Flexibility √
- Platform Options
  - ~~Commodity servers~~
  - ~~Local/cloud hybrids~~
  - ~~High security commodity servers~~
  - ~~Secure co-processors~~
  - Homomorphic crypto
  - Dedicated hardware
    - HSMs
    - FPGAs

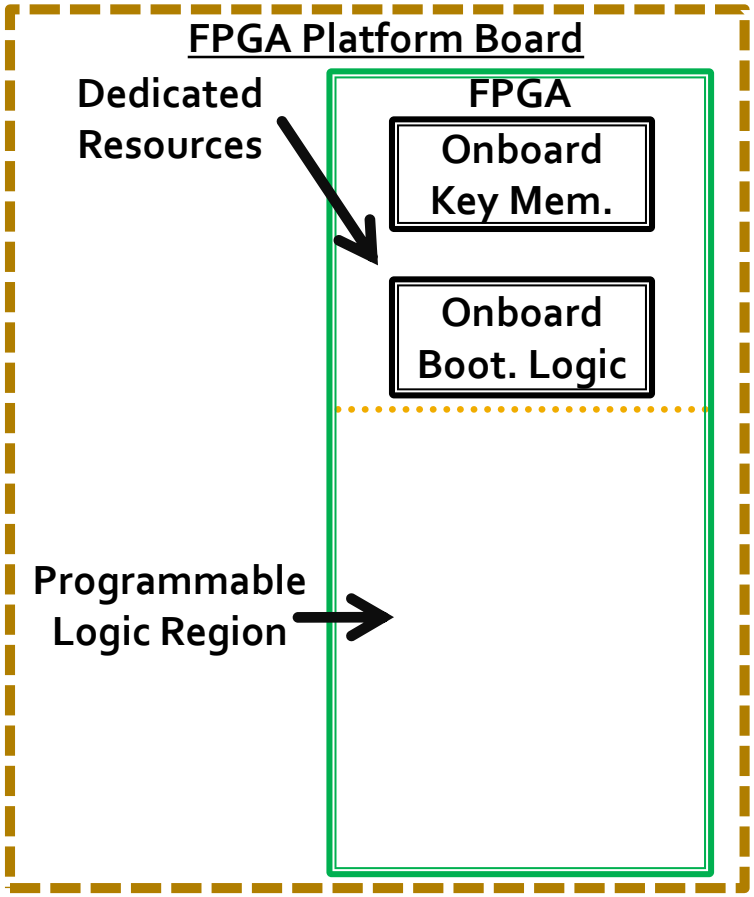
Process of Elimination

- Requirements
  - Independent administration √
  - Physically secure √
  - High performance √
  - Generality X
  - Flexibility X
- Platform Options
  - ~~Commodity servers~~
  - ~~Local/cloud hybrids~~
  - ~~High security commodity servers~~
  - ~~Secure co-processors~~
  - ~~Homomorphic crypto~~
  - Dedicated hardware
    - HSMs
    - FPGAs

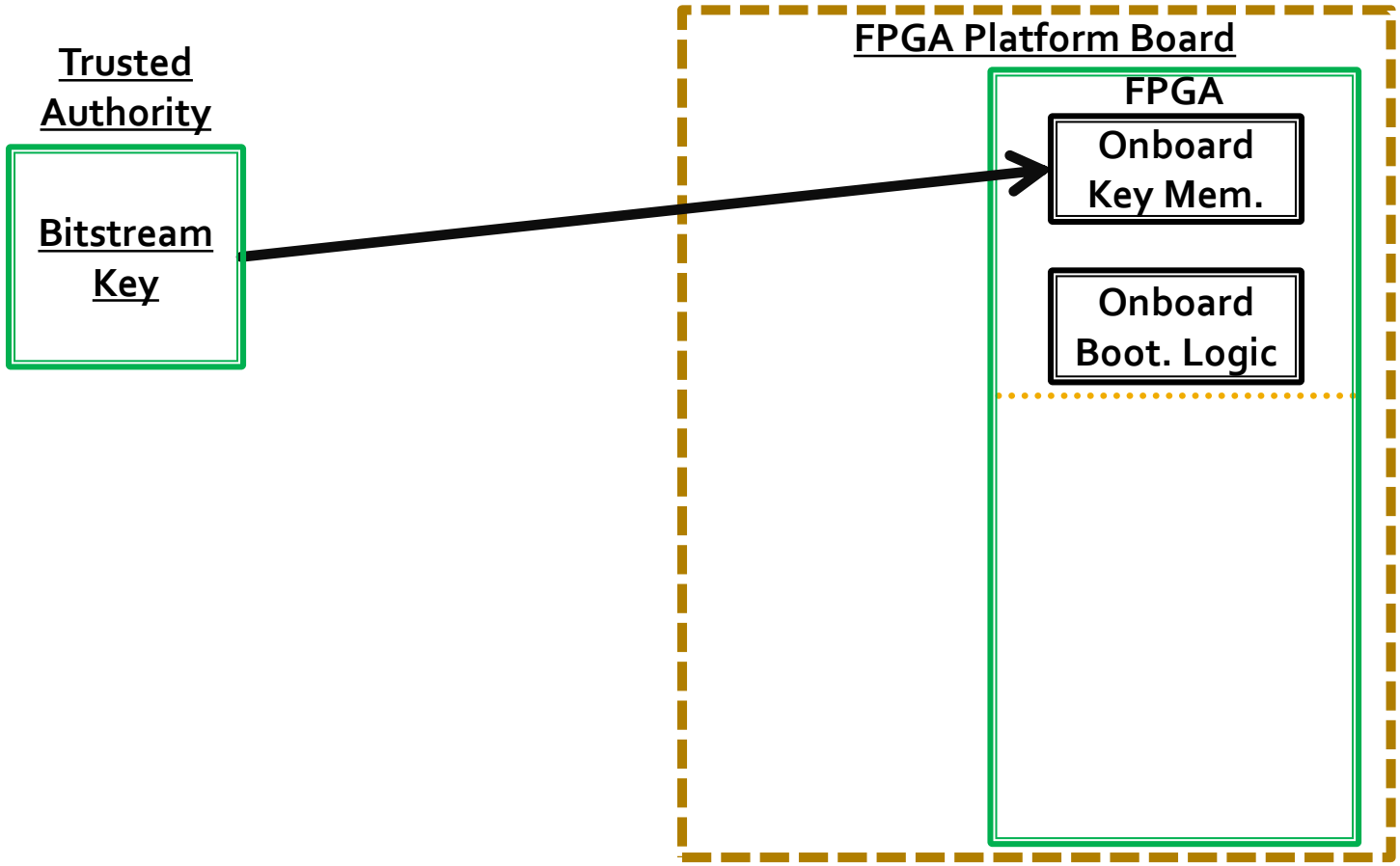
Process of Elimination

- Requirements
  - Independent administration √
  - Physically secure √
  - High performance √
  - Generality √
  - Flexibility √
- Platform Options
  - ~~Commodity servers~~
  - ~~Local/cloud hybrids~~
  - ~~High security commodity servers~~
  - ~~Secure co-processors~~
  - ~~Homomorphic crypto~~
  - Dedicated hardware
    - ~~HSMs~~
    - FPGAs

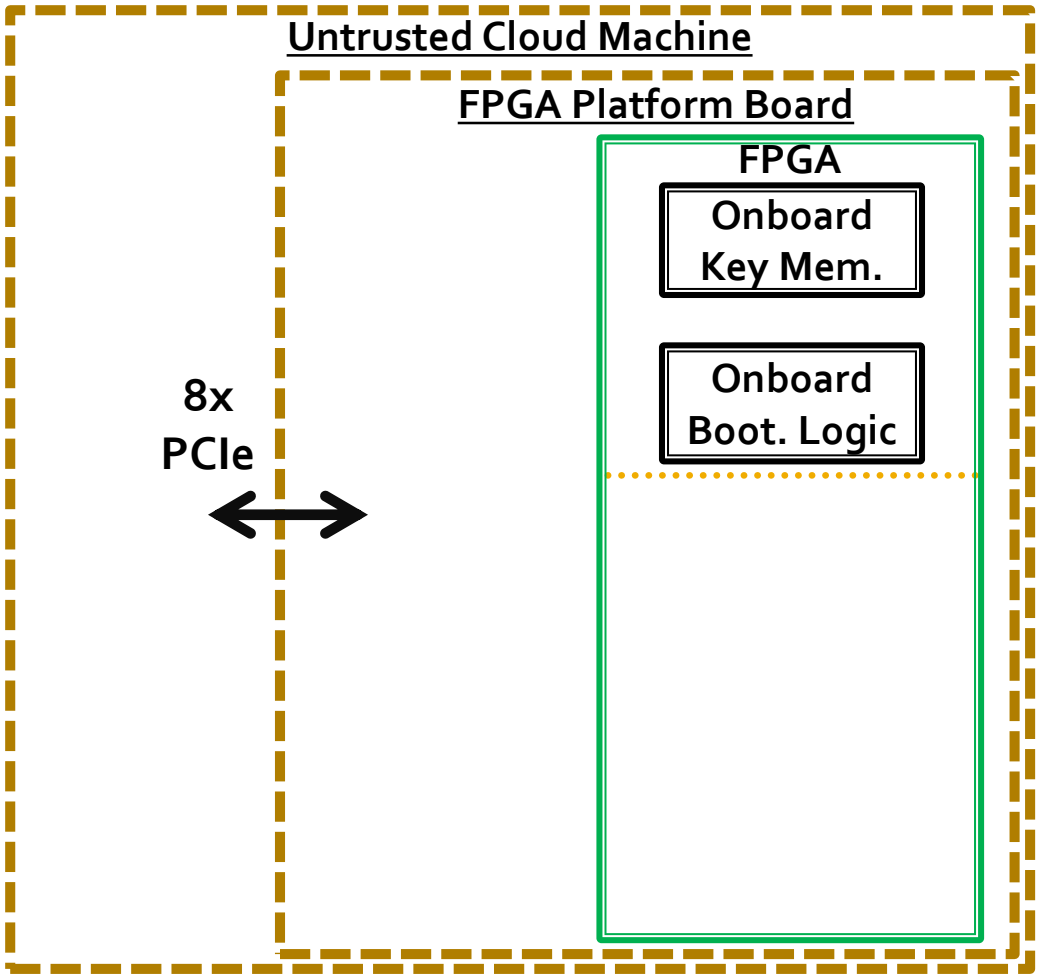
Infrastructure Setup



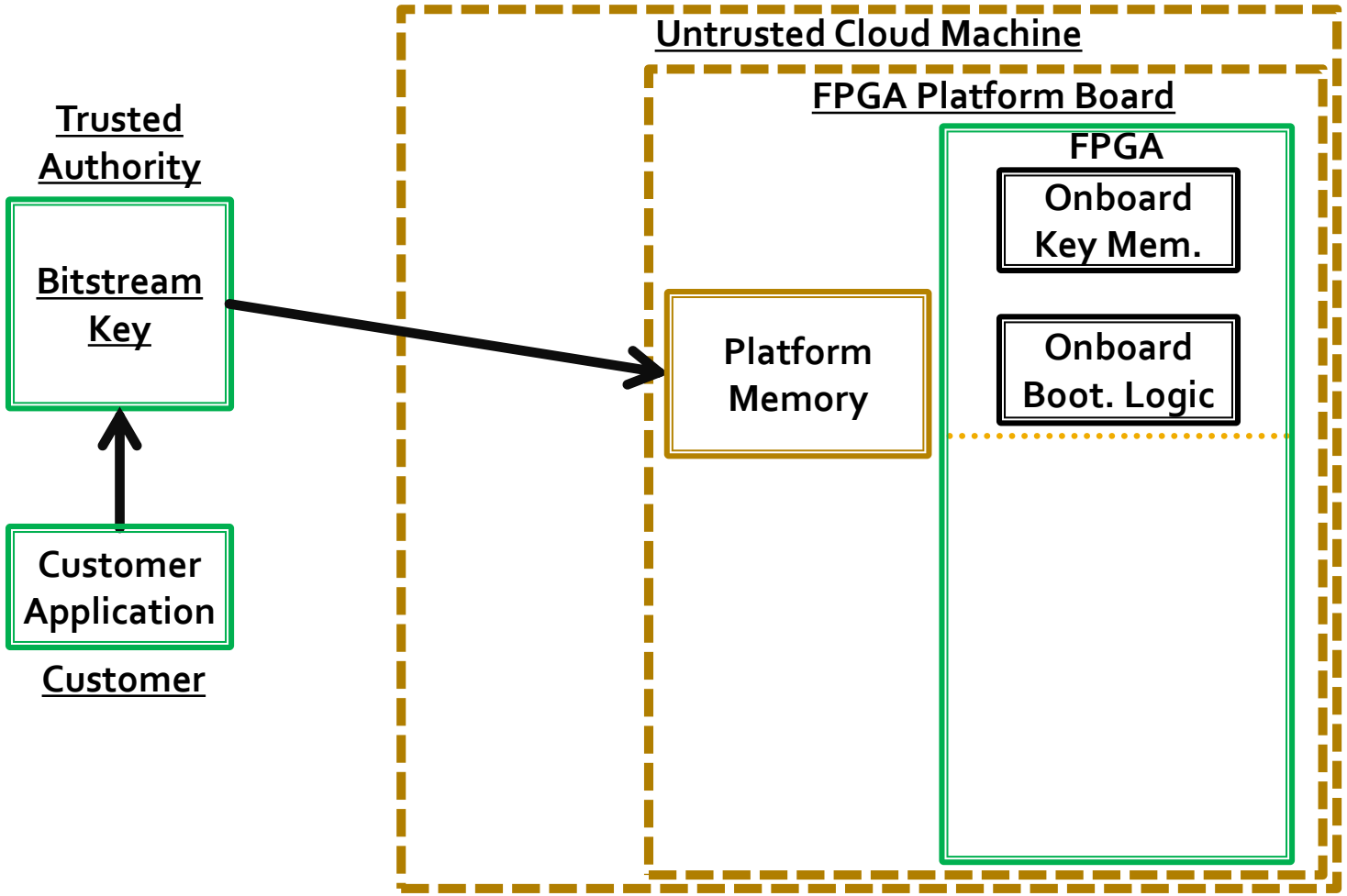
Infrastructure Setup



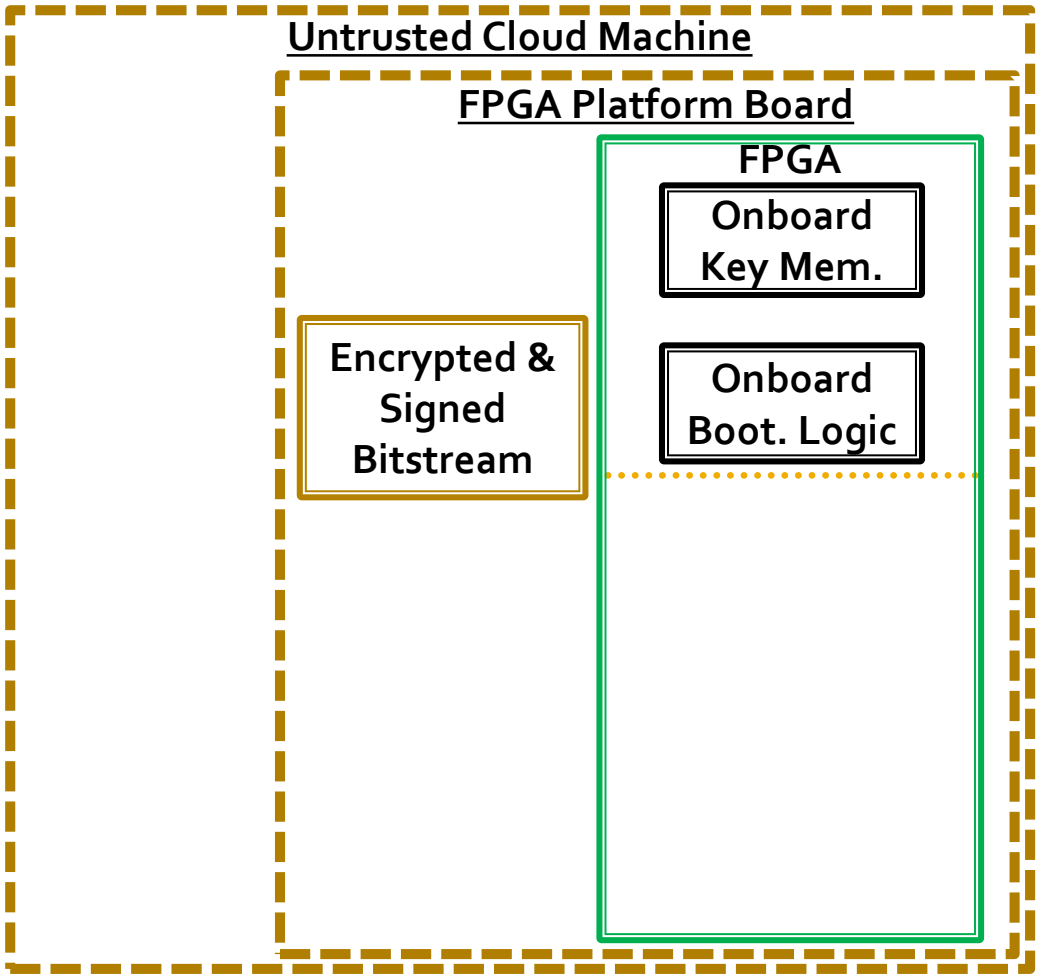
Infrastructure Setup



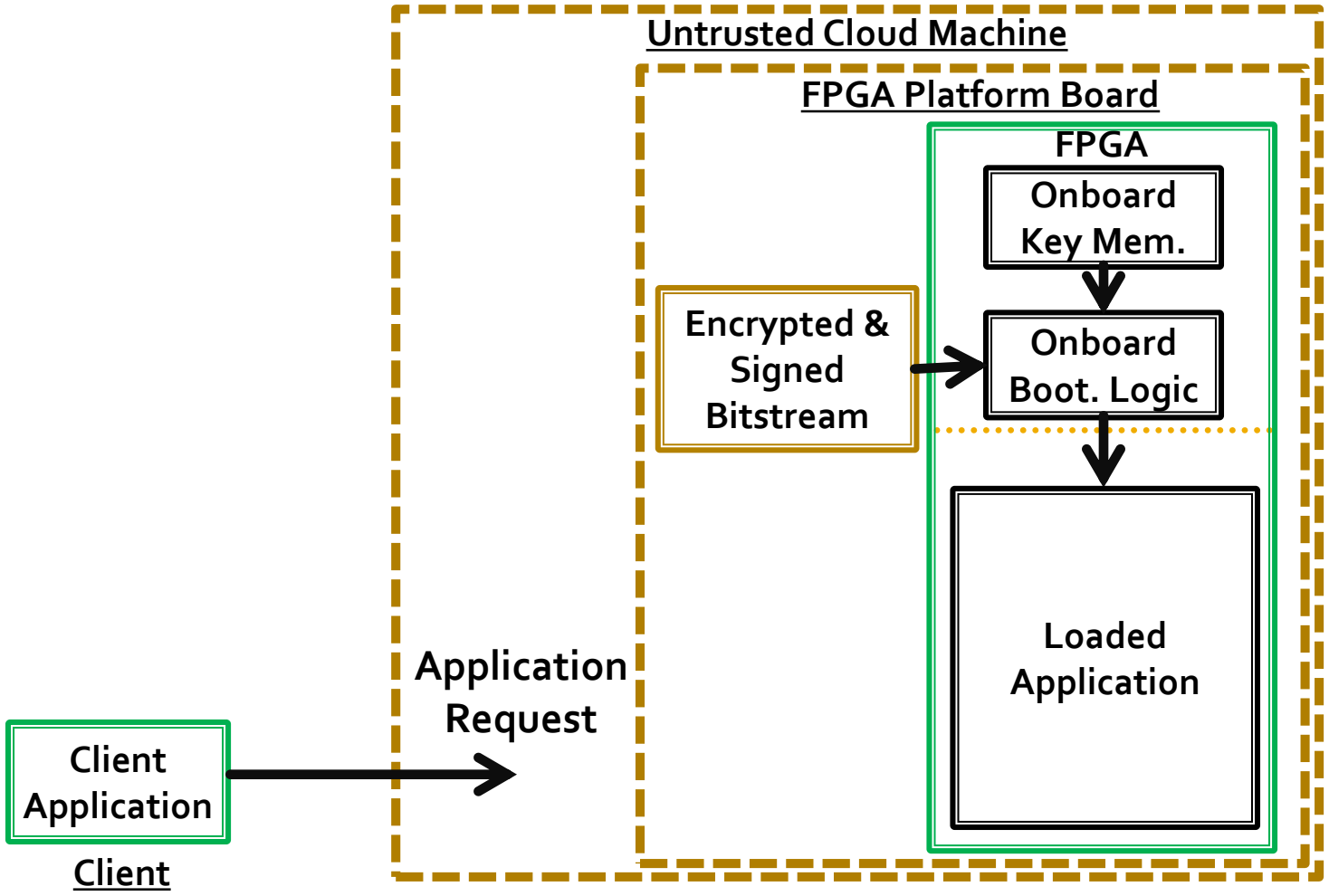
Loading Application Binaries



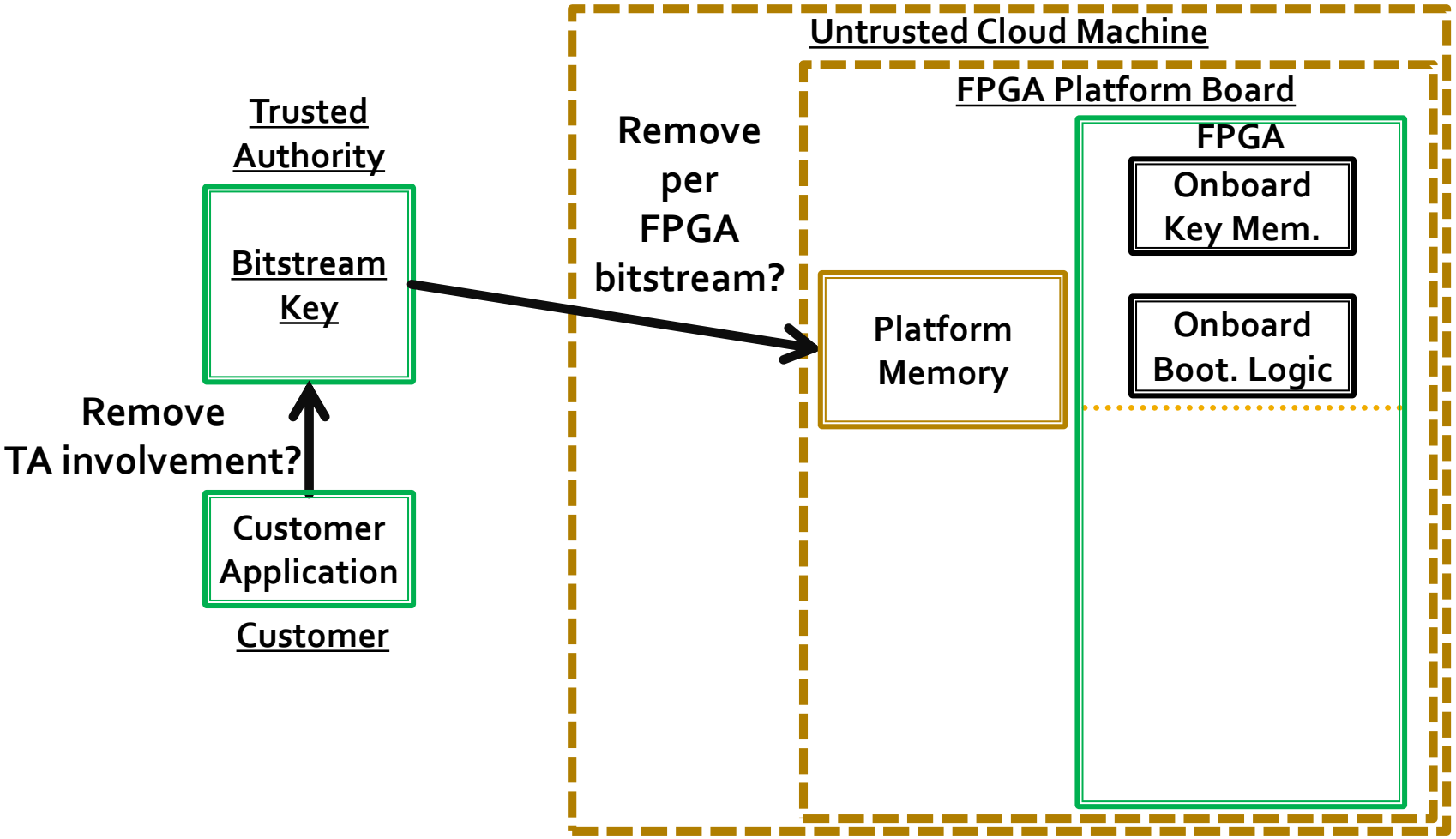
Loading Application Binaries



Dynamic Deployment

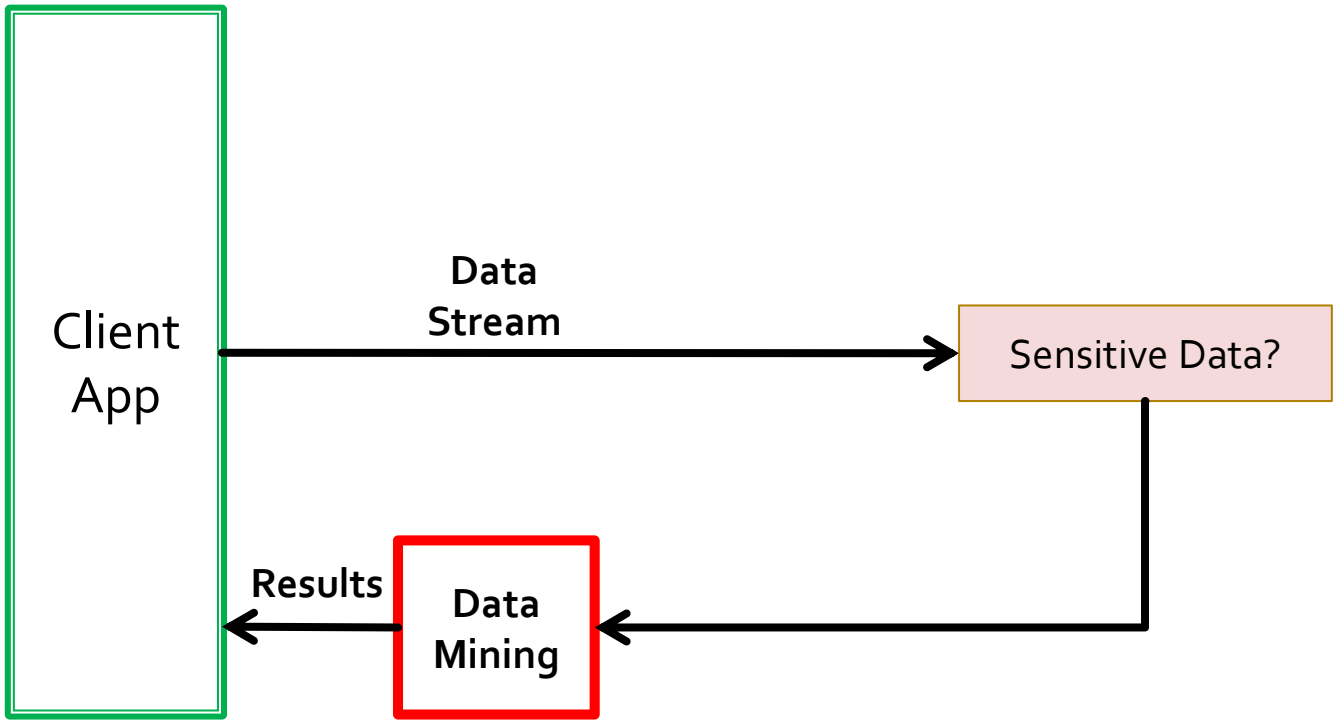


Advanced Issues – TA Interaction



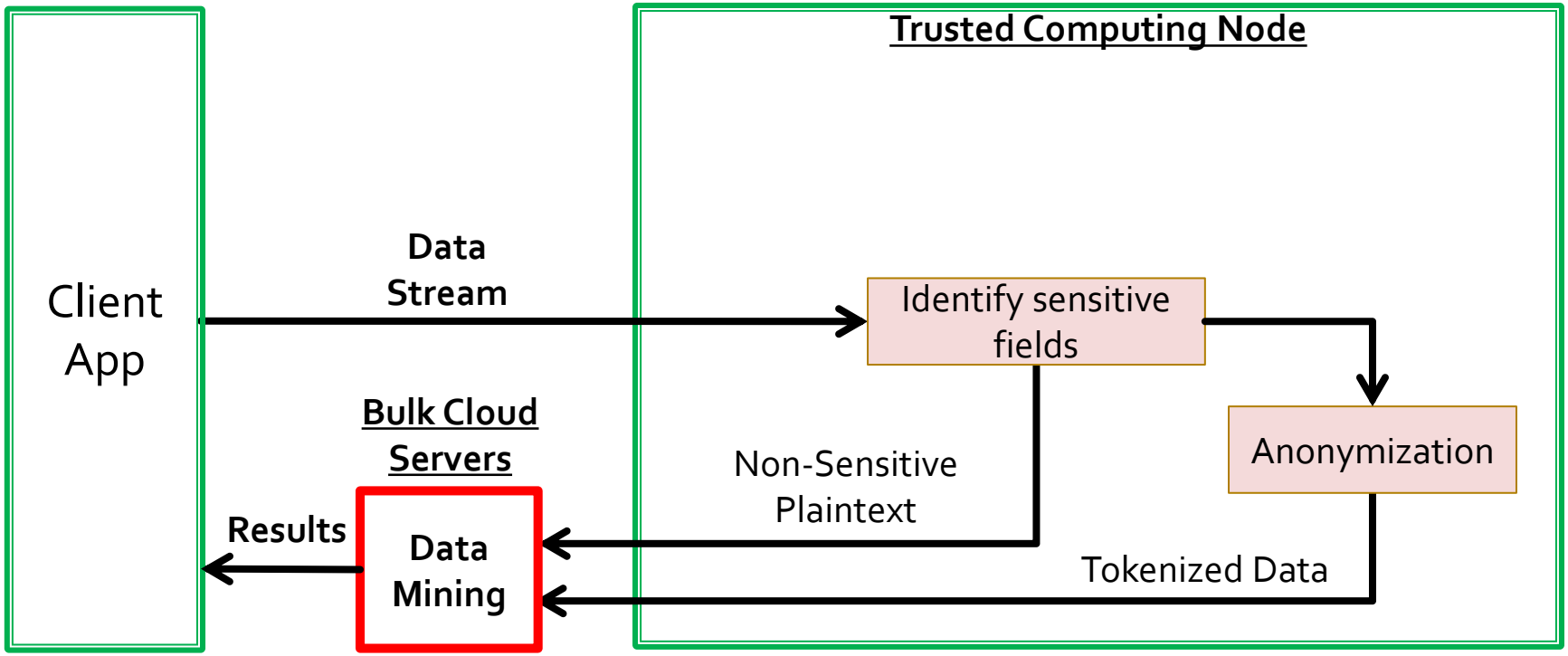
Medical record tokenization

- Sensitive vs. non-sensitive data



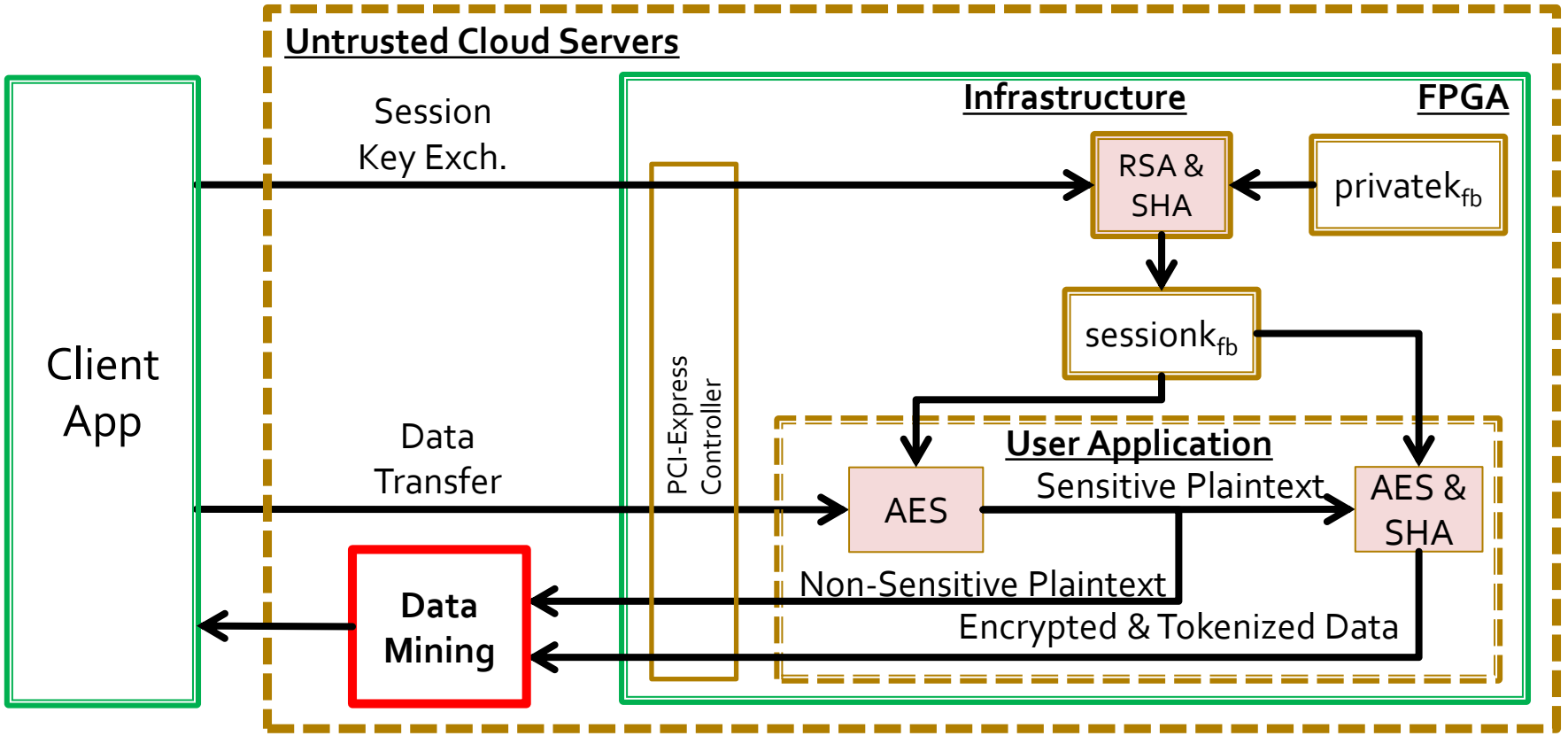
Medical record tokenization

- Sensitive vs. non-sensitive data
- Separate, tokenize & encrypt sensitive fields



Medical record tokenization

- Prototype cloud server & FPGA architecture



Resource Requirements

- On an ML605 (V6 LX 240T)

	LUTs	FF	BRAM	DSP
Full system	**18.1%**	**9%**	**6.9%**	**0.5%**
Infrastructure (RSA, SHA, PCIe, DDR3)	14.8%	8.6%	5.2%	0.5%
Tokenization (AES, AES + SHA)	3.3%	0.3%	0.7%	0.0%

Performance

- On an ML605 (V6 LX 240T)
  - 200MHz clock
  - Initiate 13+ RSA secure session key exchanges per second
  - Decrypt AES at 572MB/s
  - Tokenize with SHA-256 at 12MB/s
- Gb Ethernet is 125MB/s
- 1-10% of the incoming data was sensitive

Conclusions

- Security is paramount to the cloud
- Existing server are insufficient
- FPGAs provide native support for secure boot and secure operation
- This represents a brand new market for FPGAs