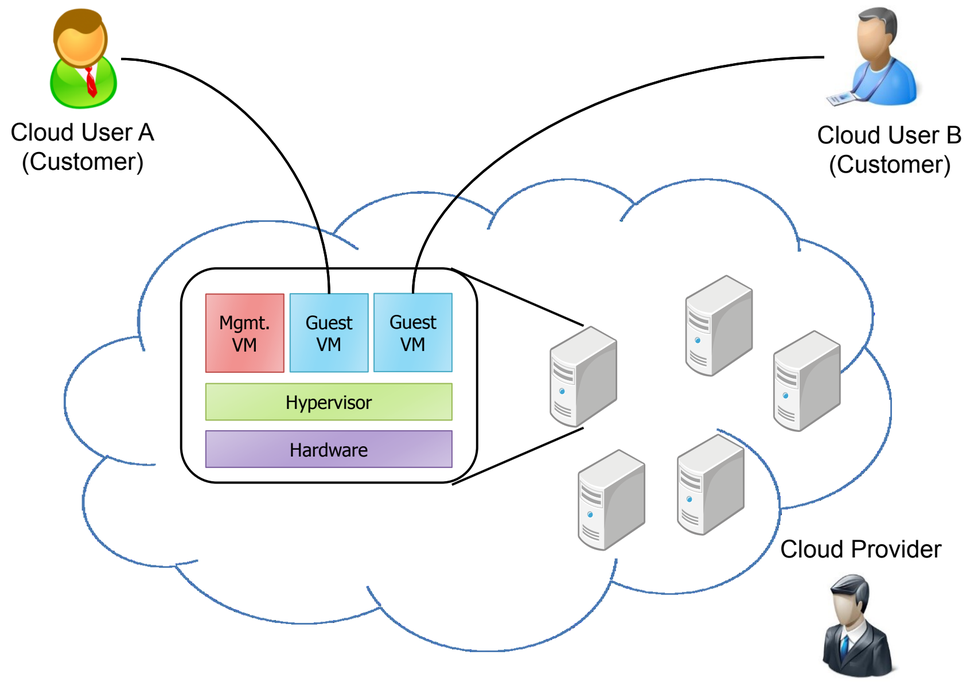
Secure Storage Service for IaaS Cloud Users

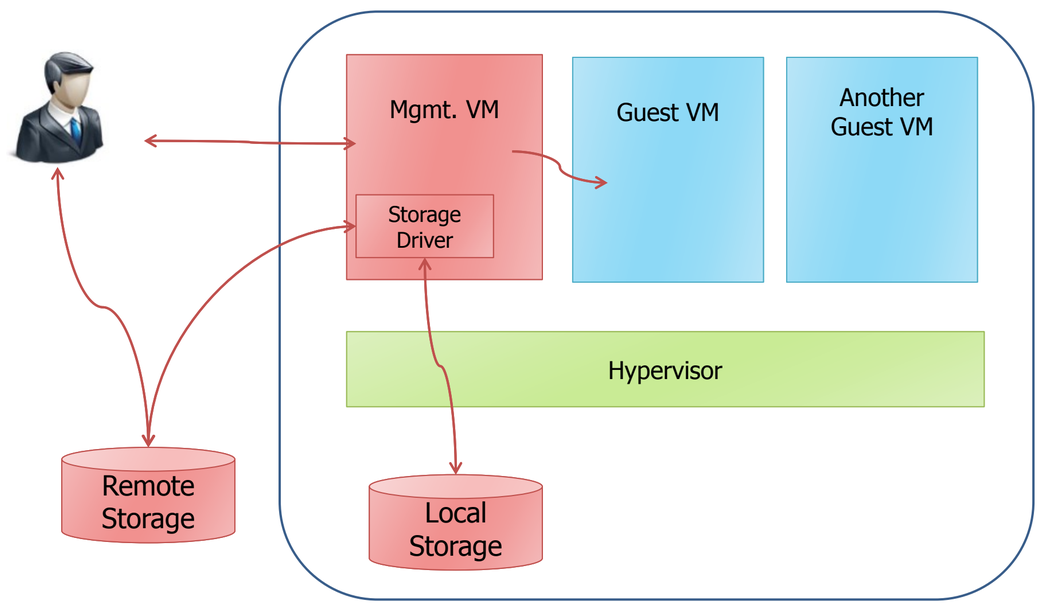
Jinho Seol, Seongwook Jin, and Seungryoul Maeng
Computer Science Department
KAIST

Background



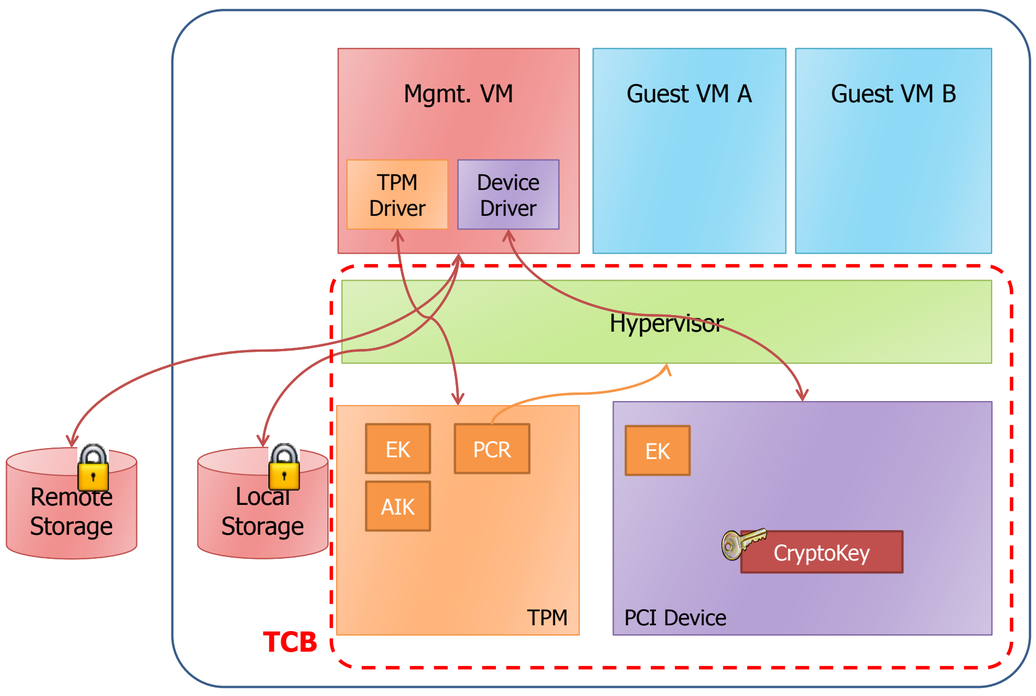
- IaaS
  - A type of cloud computing model, where cloud providers offer virtual machines including processing, network, and storage
- Challenging problems in IaaS cloud computing
  - Security concern
    - Attacks from the Internet
    - Attacks from the cloud environment

Threat Model

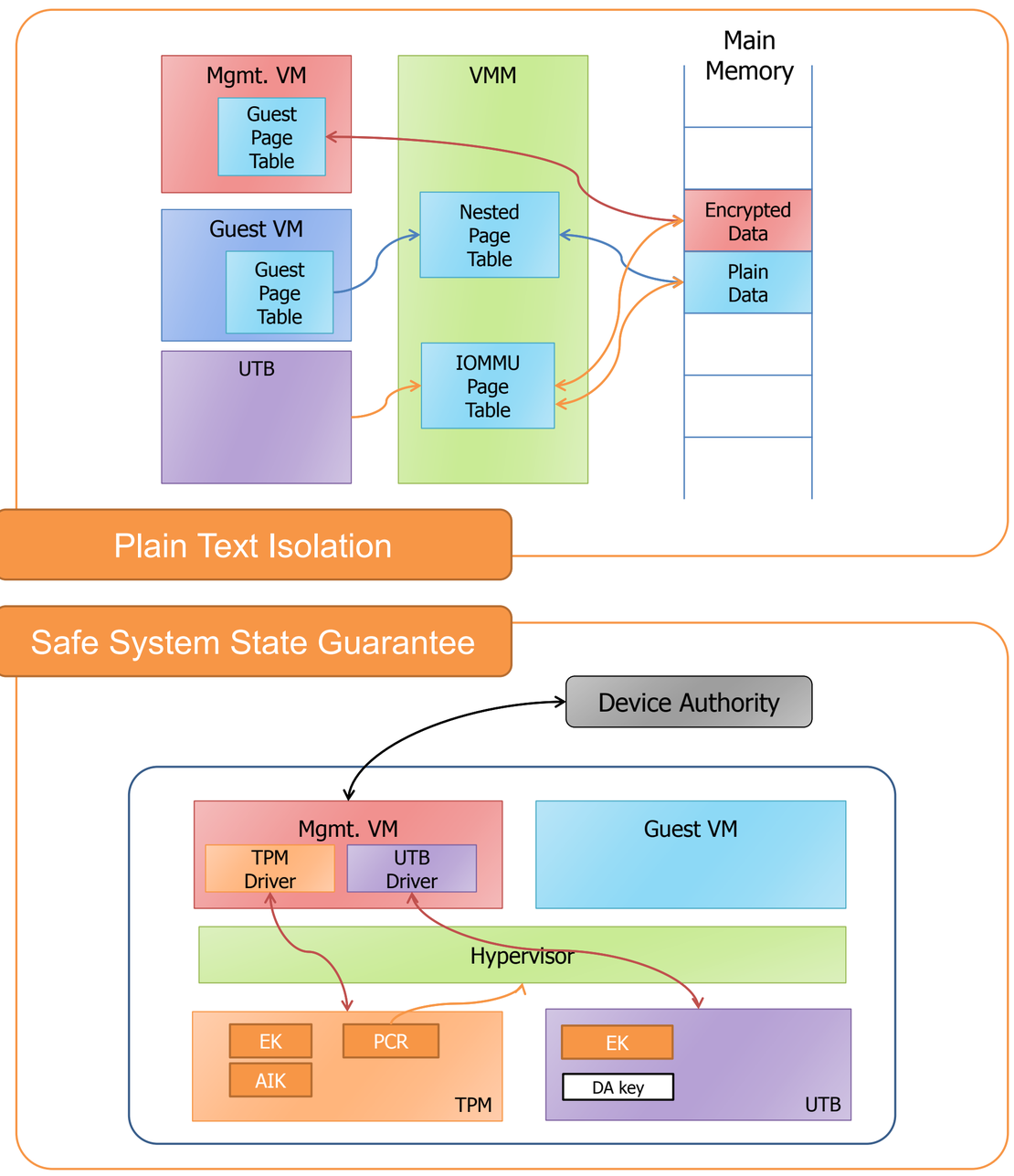


- Privileged access by a rogue administrator or a remote hacker
  - Illegal access to remote / local storages
  - Illegal access during cryptographic operations

Design Overview



- PCI typed crypto-processor
  - Cryptographic key storage
  - Isolated cryptographic operations
- Challenges
  - Plain text isolation
    - Plain text should not be loaded in mgmt. domain memory
  - Safe system state guarantee
    - Attempt to decrypt with illegal SW



Contact Information :
Jinho Seol (jhseol@calab.kaist.ac.kr)