Rocky: Replicating Block Devices for Tamper and Failure Resistant Edge-based Virtualized Desktop Infrastructure

Beom Heyn Kim
University of Toronto

Hyoungshick Kim
Sungkyunkwan University

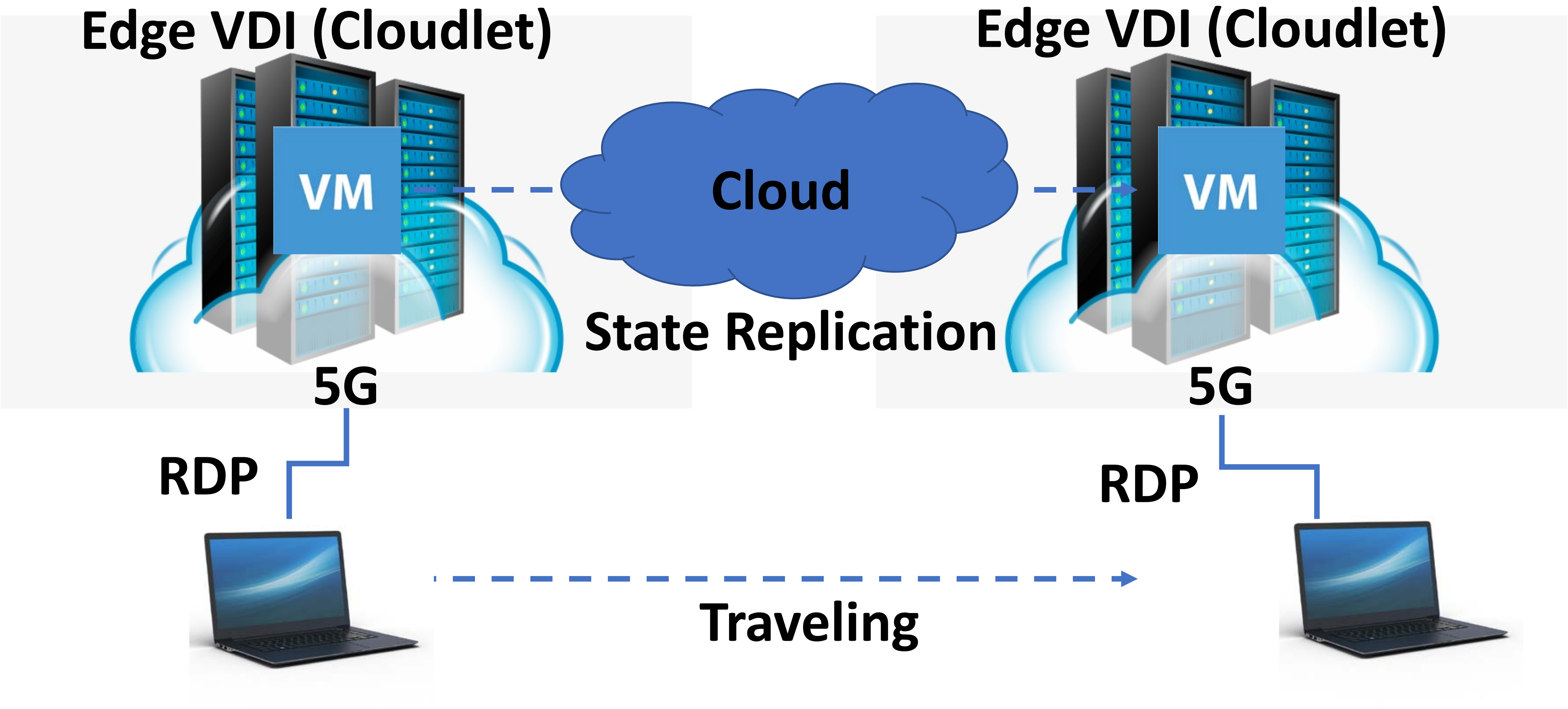
Background

Citrix Virtual Apps
and Desktops

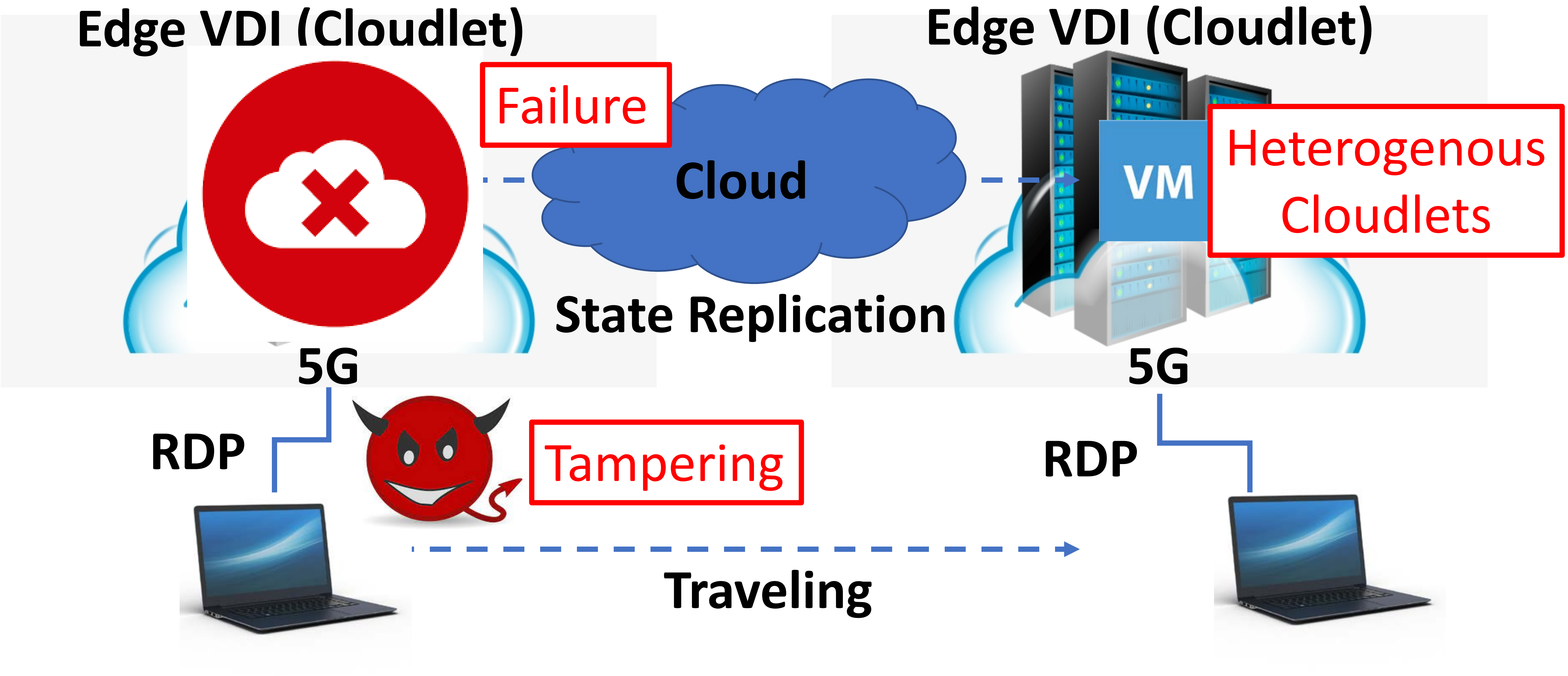
- Various VDI solutions exist and widely deployed
- The VDI market size is expected to reach 38.41 billion US Dollars by 2027 (Fior Market ’21)

VDI on Cloud may entail perceivable latency

Emergence of EdgeVDI



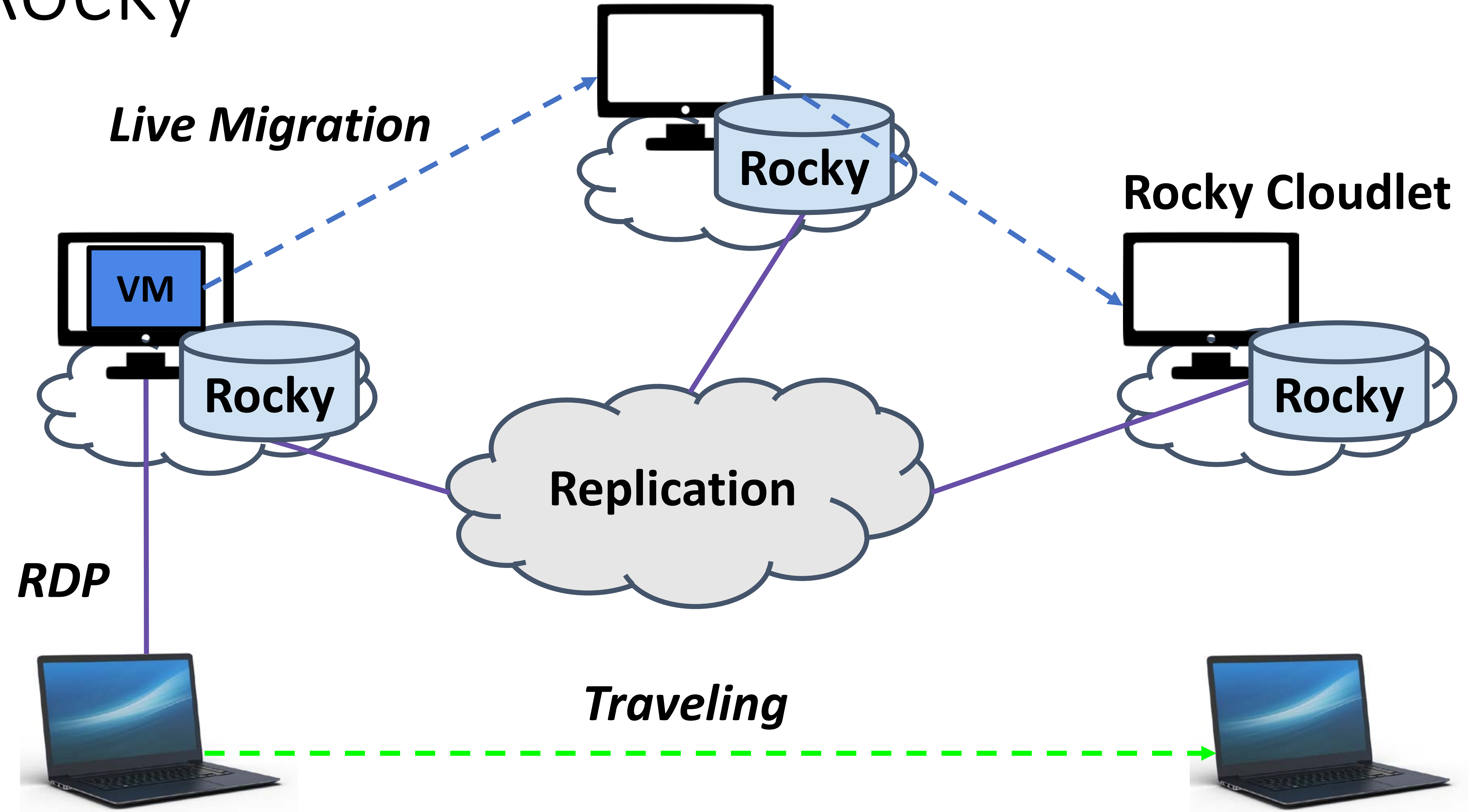
Problems with EdgeVDI



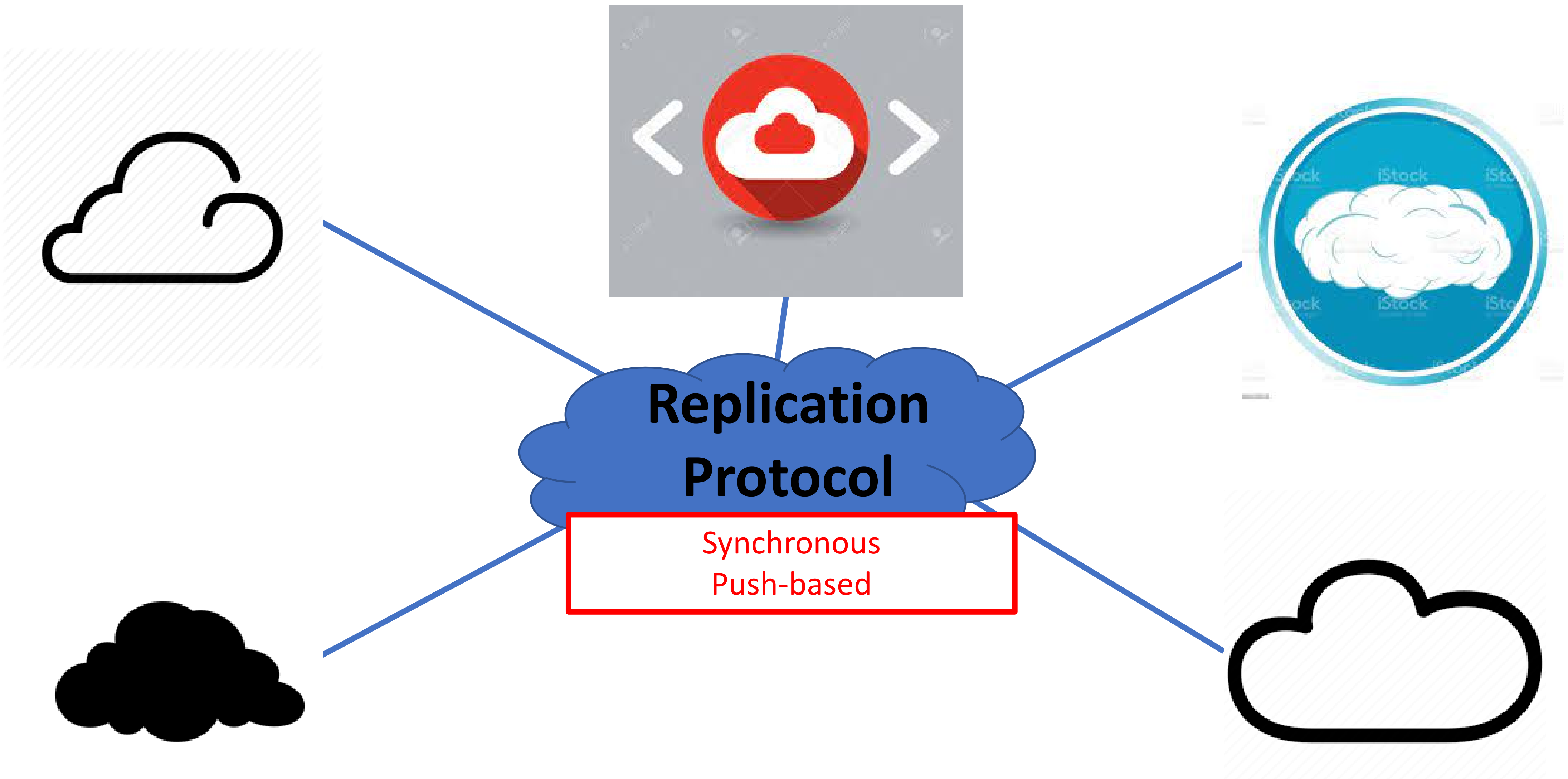
Related Works

- Ransomware detection methods.
    - But, those works do not explore how to recover tampered data.
- Tamper-resistant storage systems to protect user data against ransomware.
    - However, those works require modification on hardware architecture or need a special hardware device.
- Existing solutions against tampering attacks do not work when a cloudlet on which the VM runs fails.

Rocky


Live Migration
Rocky
Rocky Cloudlet
VM
Rocky
Rocky
Replication
RDP
Traveling

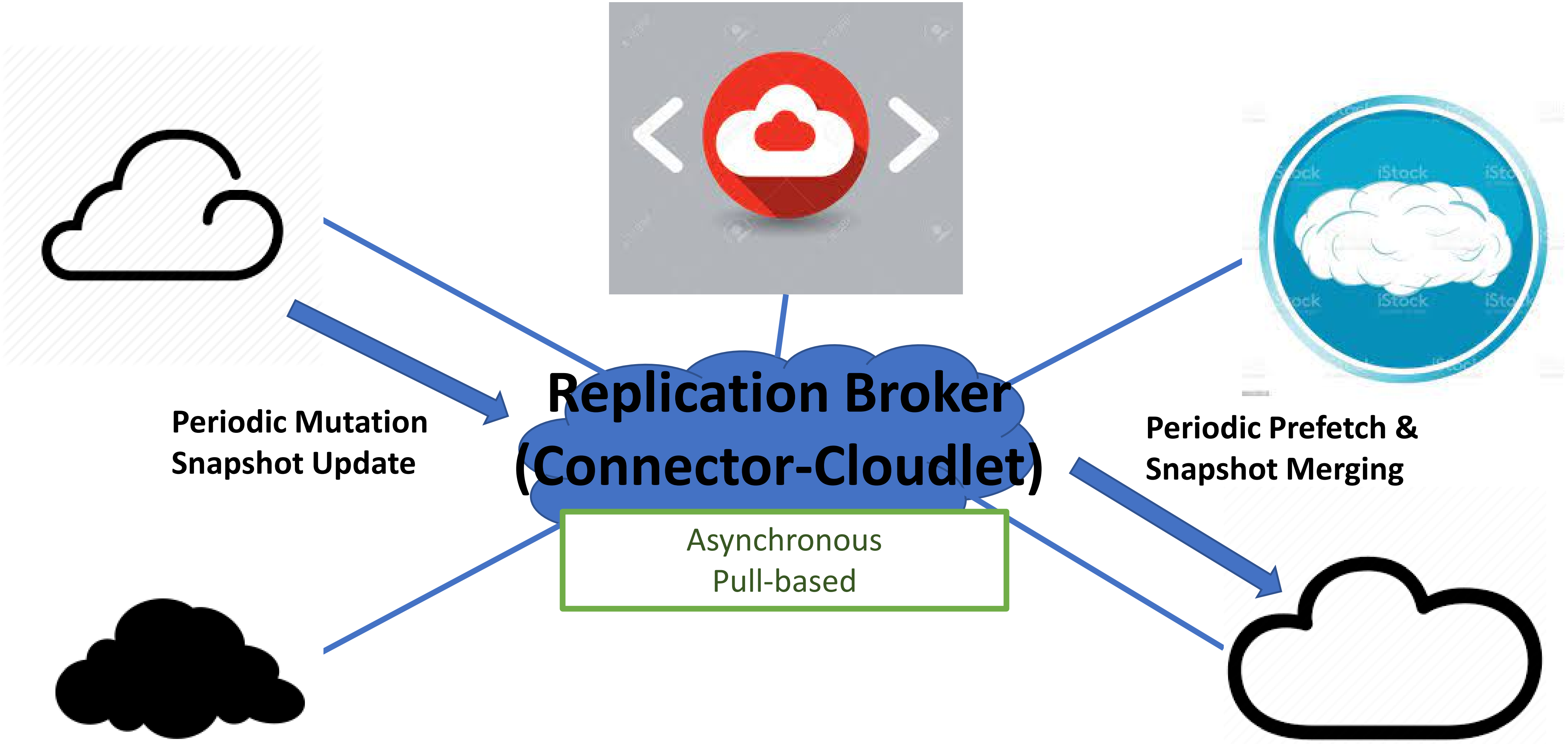
Heterogenous Cloudlets



Replication Protocol

Synchronous
Push-based

Rocky: Pub/Sub Style Replication



Replication Broker (Connector-Cloudlet)

Periodic Mutation Snapshot Update

Periodic Prefetch & Snapshot Merging

Asynchronous

Pull-based

Tampering Attacks on Block Device States

Block-Level View

T1: Write(Block 1, X), Write(Block 2, Y), Write(Block 3, Z)

T2:

Ransomware Encrypts Disk Blocks

T3: Write(Block 1, E(X)), Write(Block 2, E(Y)), Write(Block 3, E(Z))

Rocky: Replay Non-Tampering Writes Only

Replay to recover

T1: Write(Block 1, X), Write(Block 2, Y), Write(Block 3, Z)

↓

T2:

Ransomware Encrypts Disk Blocks

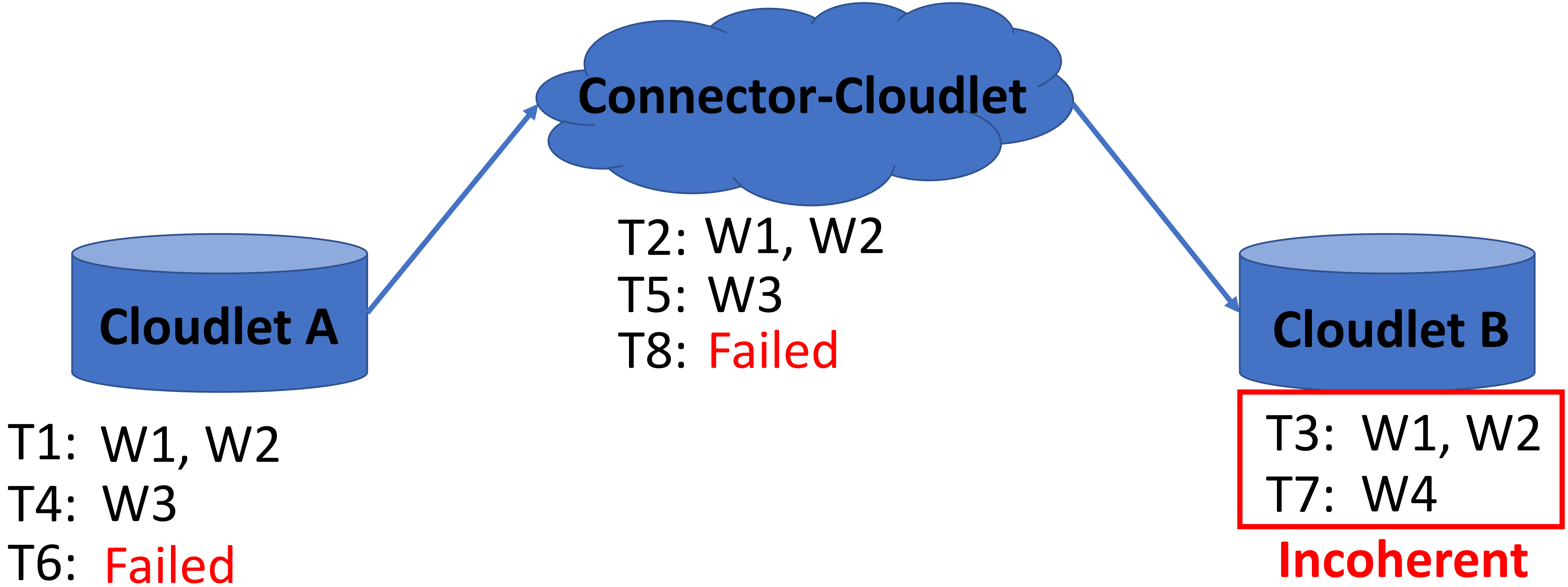
Anti-malware can detect tampering attacks and inform

↓

T3: Write(Block 1, E(X)), Write(Block 2, E(Y)), Write(Block 3, E(Z))

Don’t Replay

Coherency Problem



Connector-Cloudlet

T2: W1, W2
T5: W3
T8: Failed

Cloudlet A

T1: W1, W2
T4: W3
T6: Failed

Cloudlet B

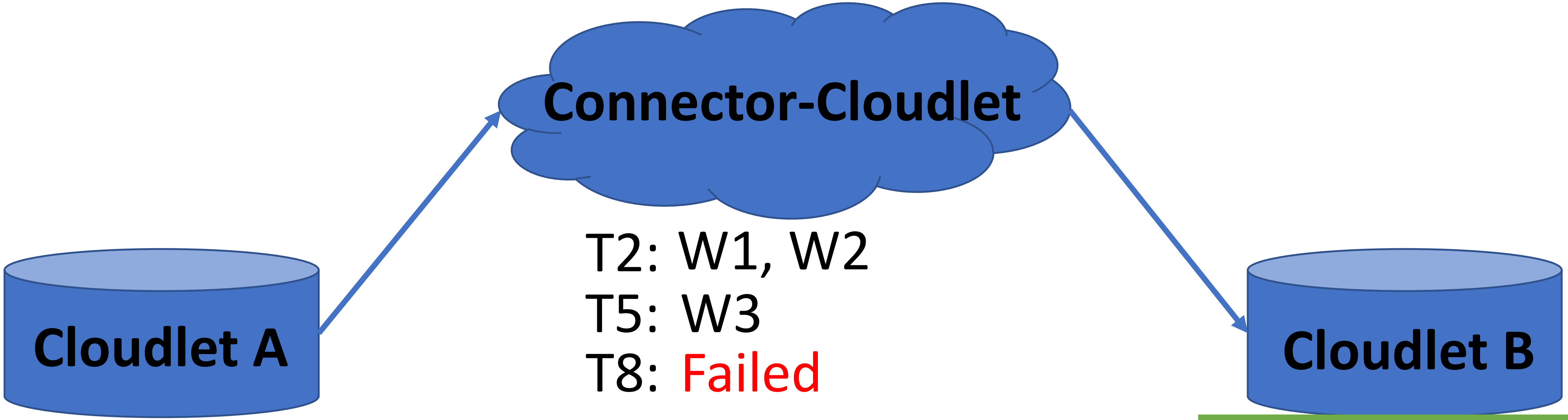
T3: W1, W2
T7: W4

Incoherent

Contiguous Write Sequence: W1, W2, W3, W4

'W3' is permanently lost!

Coherency Problem



T2: W1, W2
T5: W3
T8: Failed

T1: W1, W2
T4: W3
T6: Failed

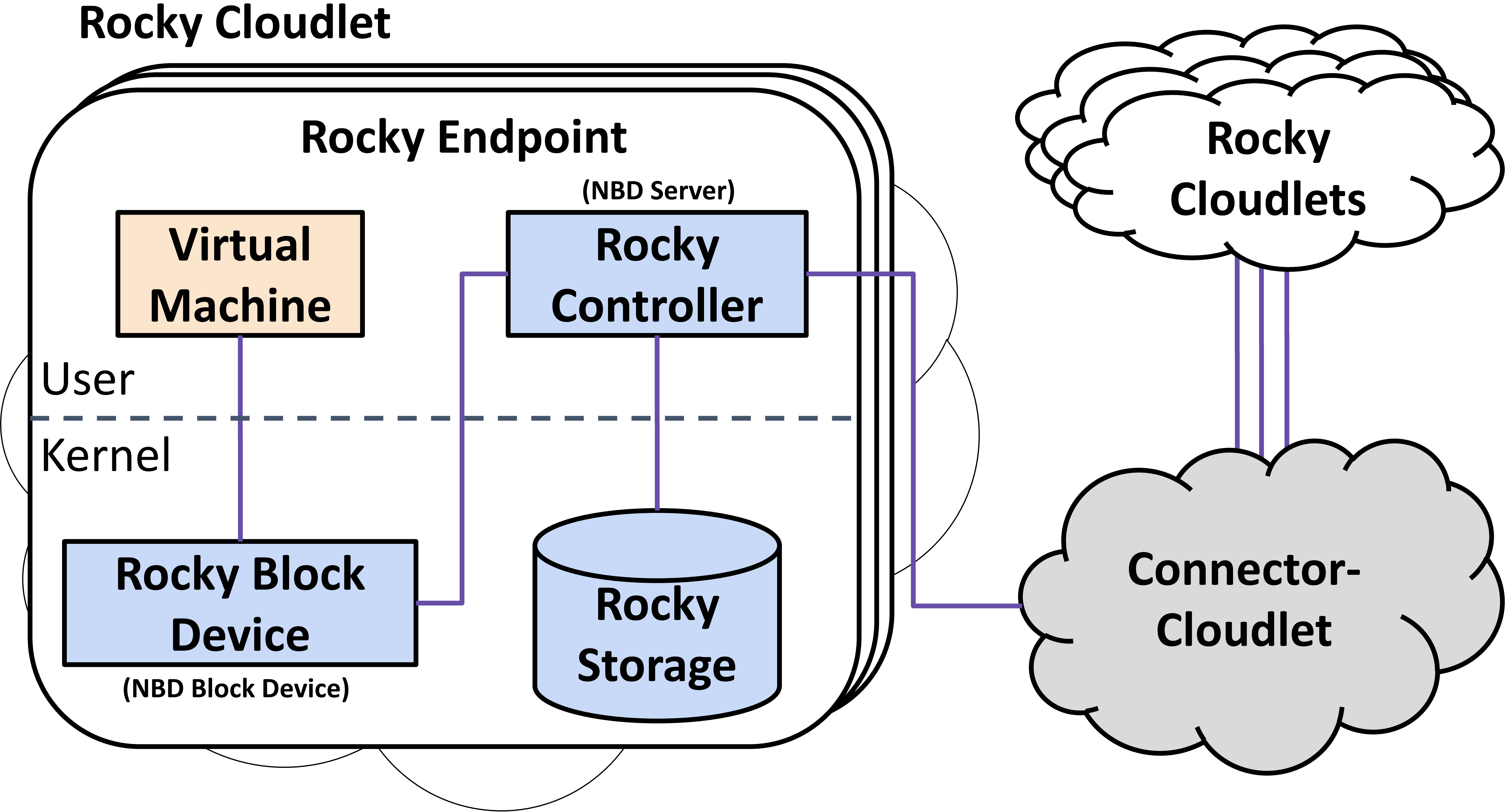
Coherent

T3: W1, W2
T7: W4

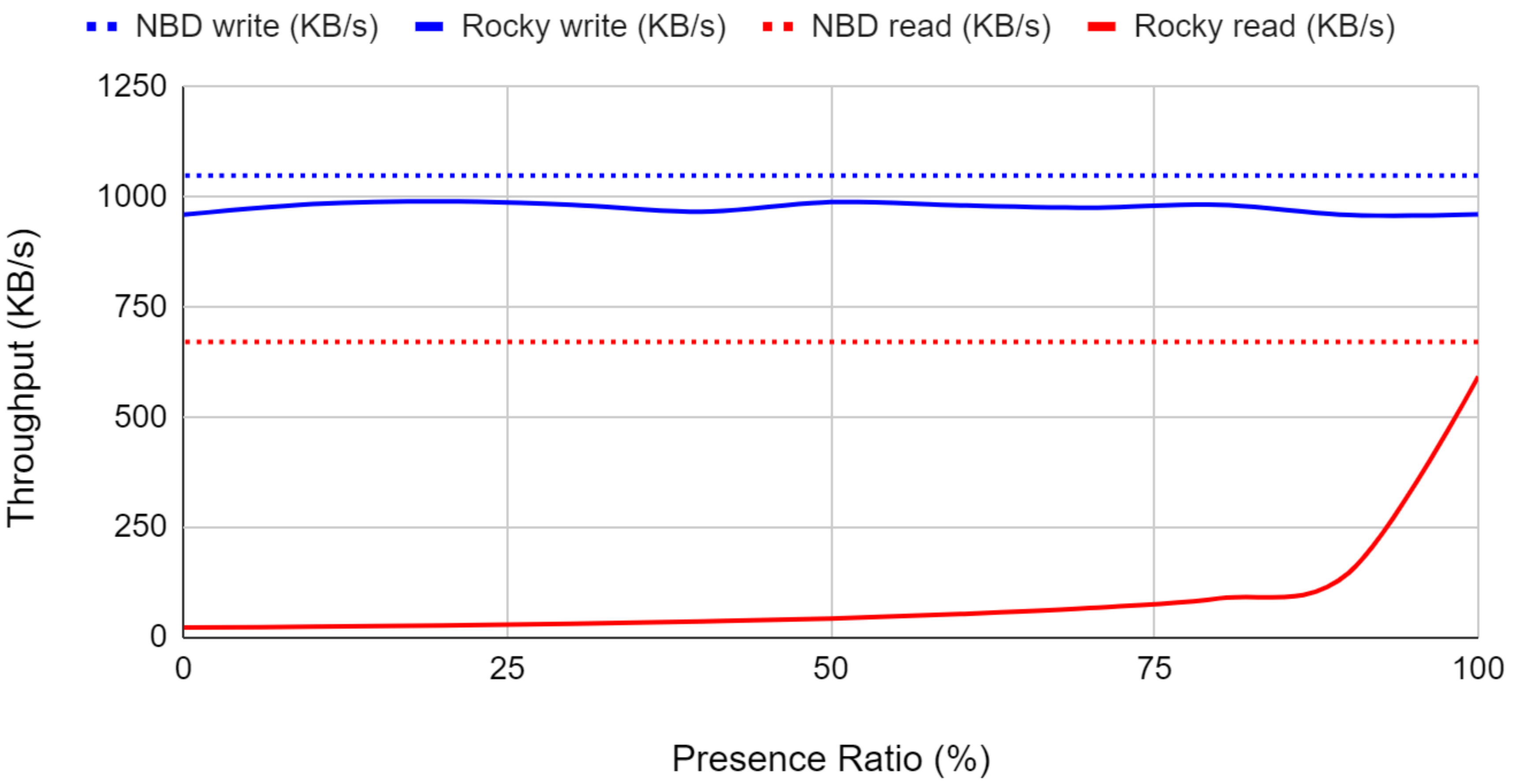
Incoherent

Contiguous Write Sequence: W1, W2, W3, W4

Discard W4 and Replay W1 and W2 only


Rocky Cloudlet
Rocky Endpoint
(NBD Server)
Virtual Machine
Rocky Controller
User
Kernel
Rocky Block Device
(NBD Block Device)
Rocky Storage
Rocky Cloudlets
Connector-Cloudlet

Performance Overhead



- If up-to-date blocks are replicated timely, only 8.4% and 11.9% additional throughput overheads are required for write and read, respectively.

Conclusion

Heterogenous Cloudlets

- Pub/Sub Style Replication Protocol

Tampering

- Replaying Non-Tampering Writes

Failure

- Replaying Contiguous Writes

- **Rocky Shows that Overcoming All These Three Problems is Possible**