阿里云智能集团
ALIBABA CLOUD INTELLIGENCE GROUP

Ransom Access Memories: Achieving Practical Ransomware Protection in Cloud with DeftPunk

Zhongyu Wang, Yaheng Song, Erci Xu, Haonan Wu,
Guangxun Tong, Shizhuo Sun, Haoran Li,
Jincheng Liu, Lijun Ding, Rong Liu, Jiaji Zhu, Jiesheng Wu

ALIBABA GROUP

阿里云智能集团
ALIBABA CLOUD INTELLIGENCE GROUP

Content

01 Ransomware 101

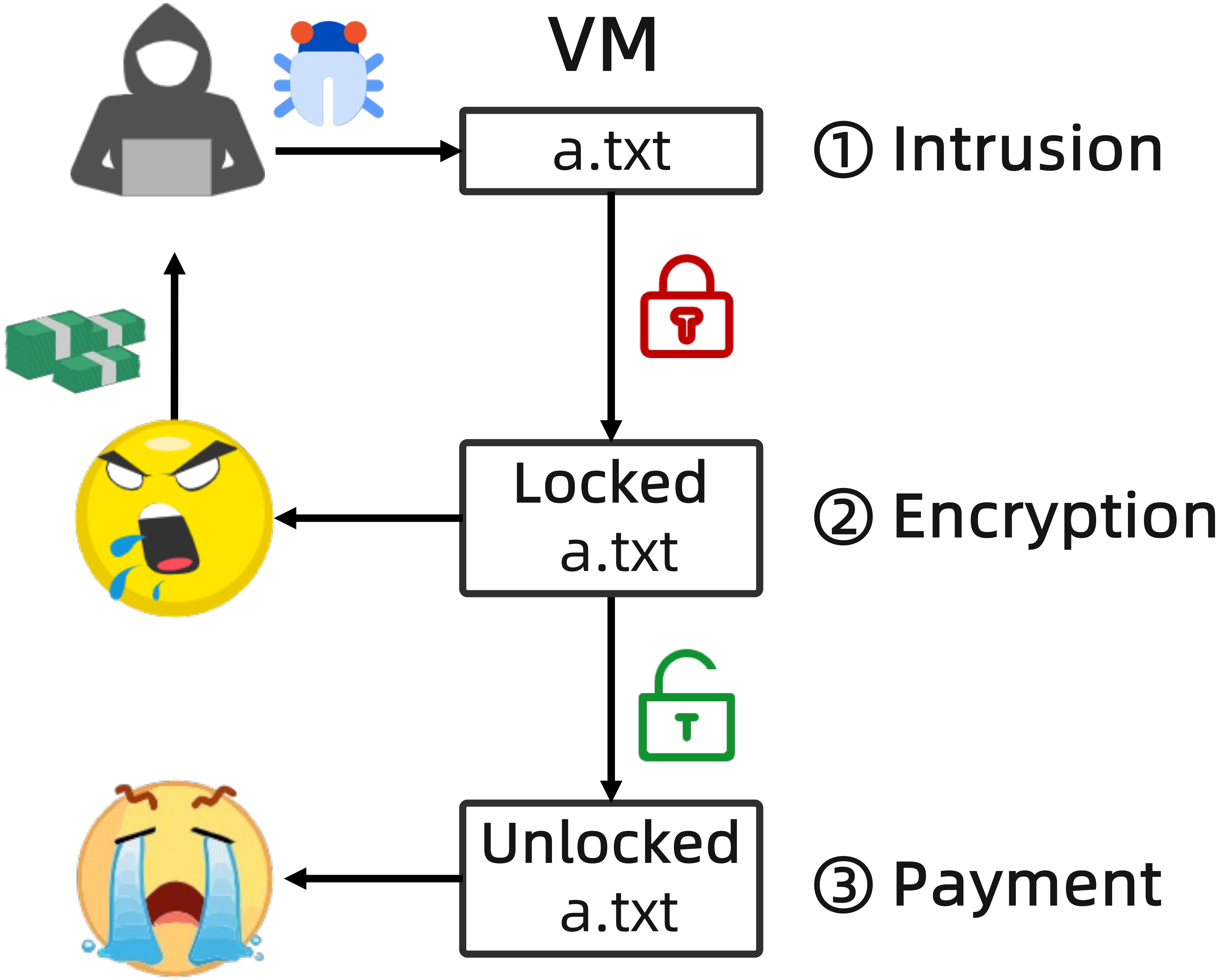
02 Common Protections

03 DeftPunk

04 Evaluation

05 Discussion

Ransomware Procedure



VM

a.txt

① Intrusion

Locked a.txt

② Encryption

Unlocked a.txt

③ Payment

zscaler

38%

Ransom incidents

SOPHOS

90%

Ransom money

Alibaba Cloud

1,000+ attacks in 2022 Q3

118% increase

Ransomware is rampant in cloud!

Content

01 Ransomware 101

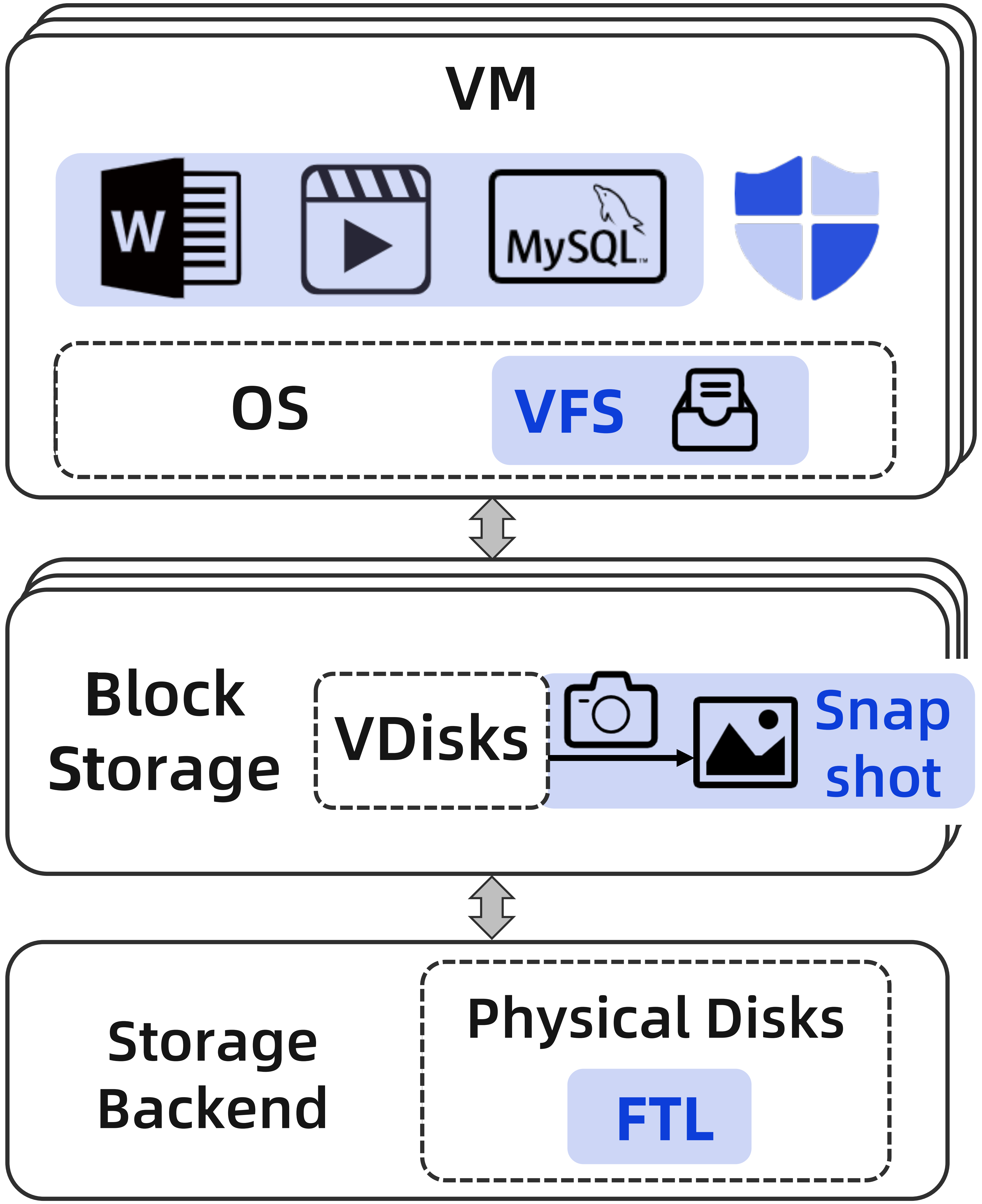
02 Common Protections

03 DeftPunk

04 Evaluation

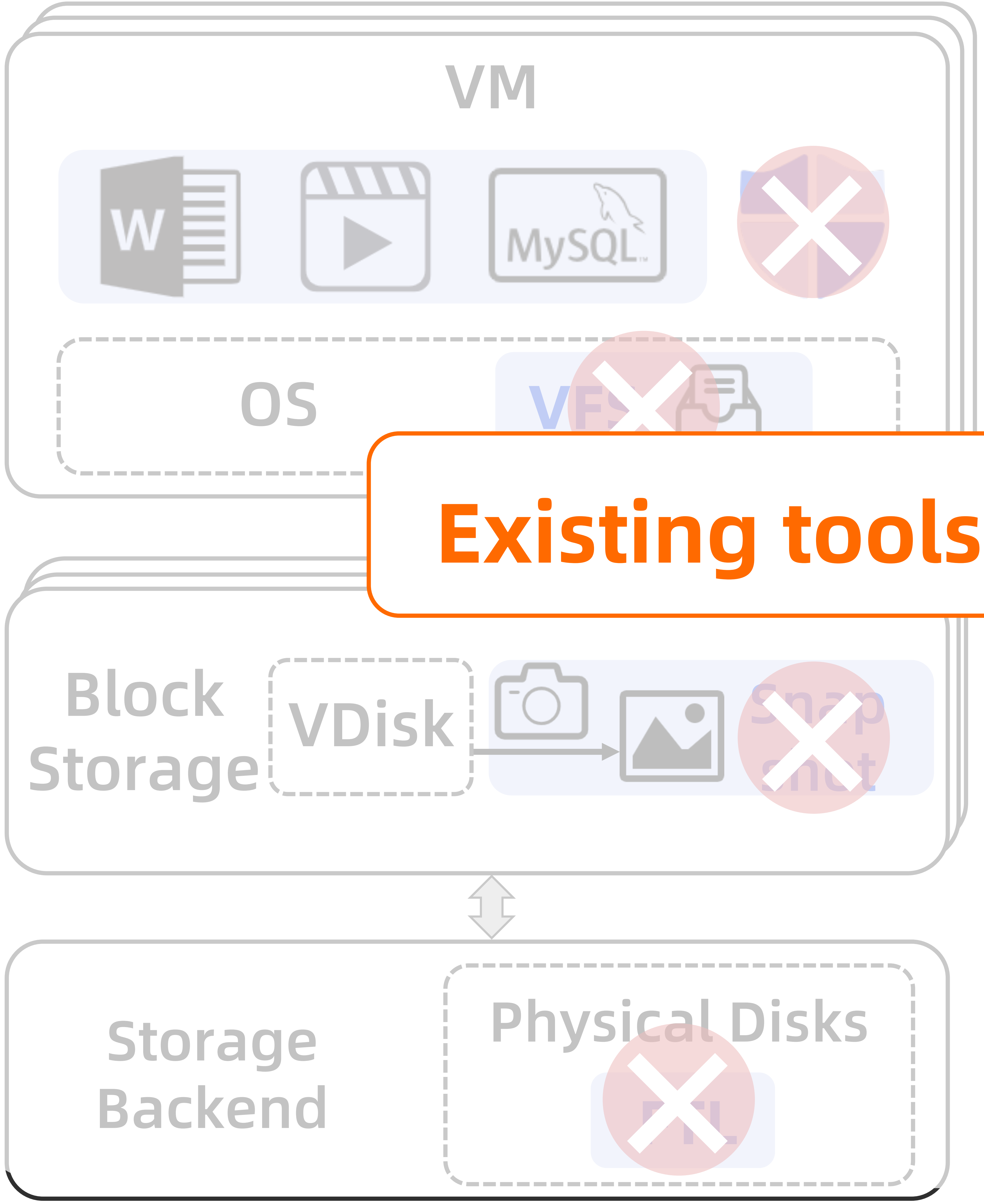
05 Discussion

Common Protections



User awareness	Anti-virus softwares
OS protetction	UNVEIL@Security’16
Scheduled snapshot	Alibaba Cloud, AWS, Azure etc.
Hardware protection	FlashGuard@CCS’17 RSSD@ASPLOS’22

Not Working in Cloud



User-awareness — Phishing, Weak Pwd., Outdated Soft.

Unpatched fficial OS

Existing tools are inapplicable for cloud!

Scheduled snapshot — $ Costly, Data Loss

Hardware protection — coming soon

Content

01 Ransomware 101

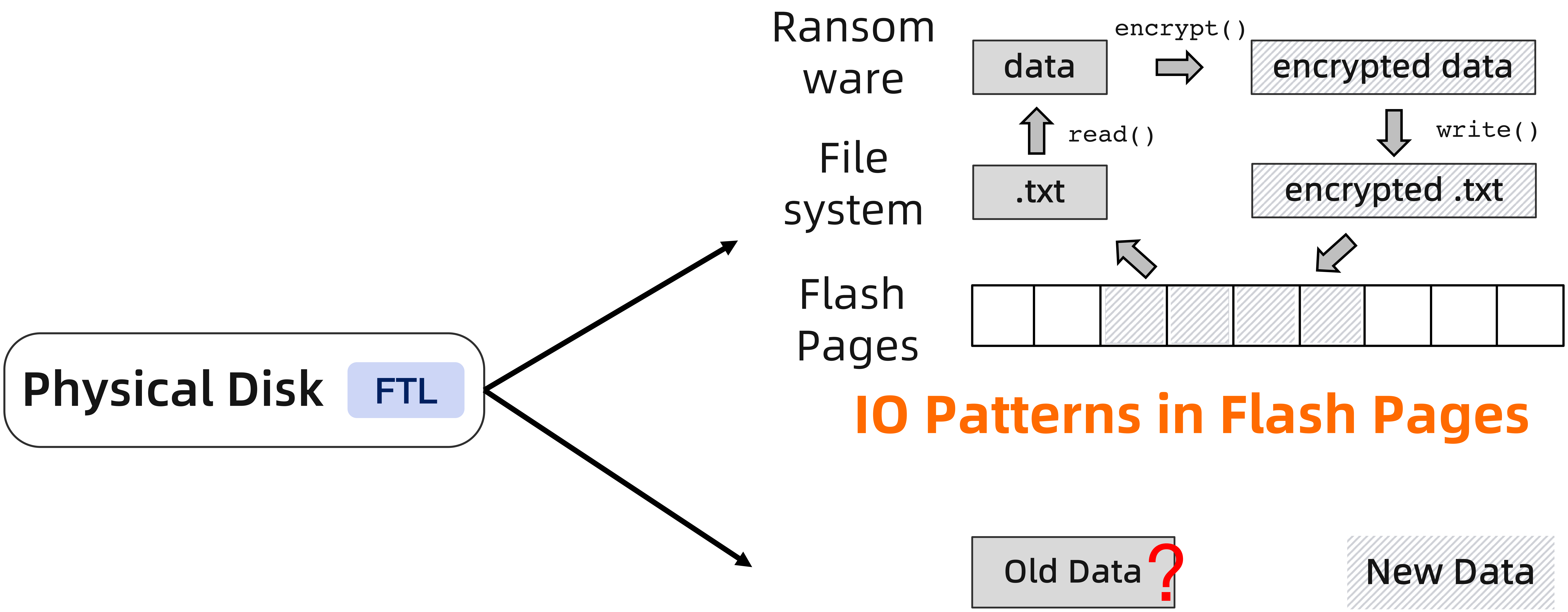
02 Common Protections

03 DeftPunk

04 Evaluation

05 Discussion

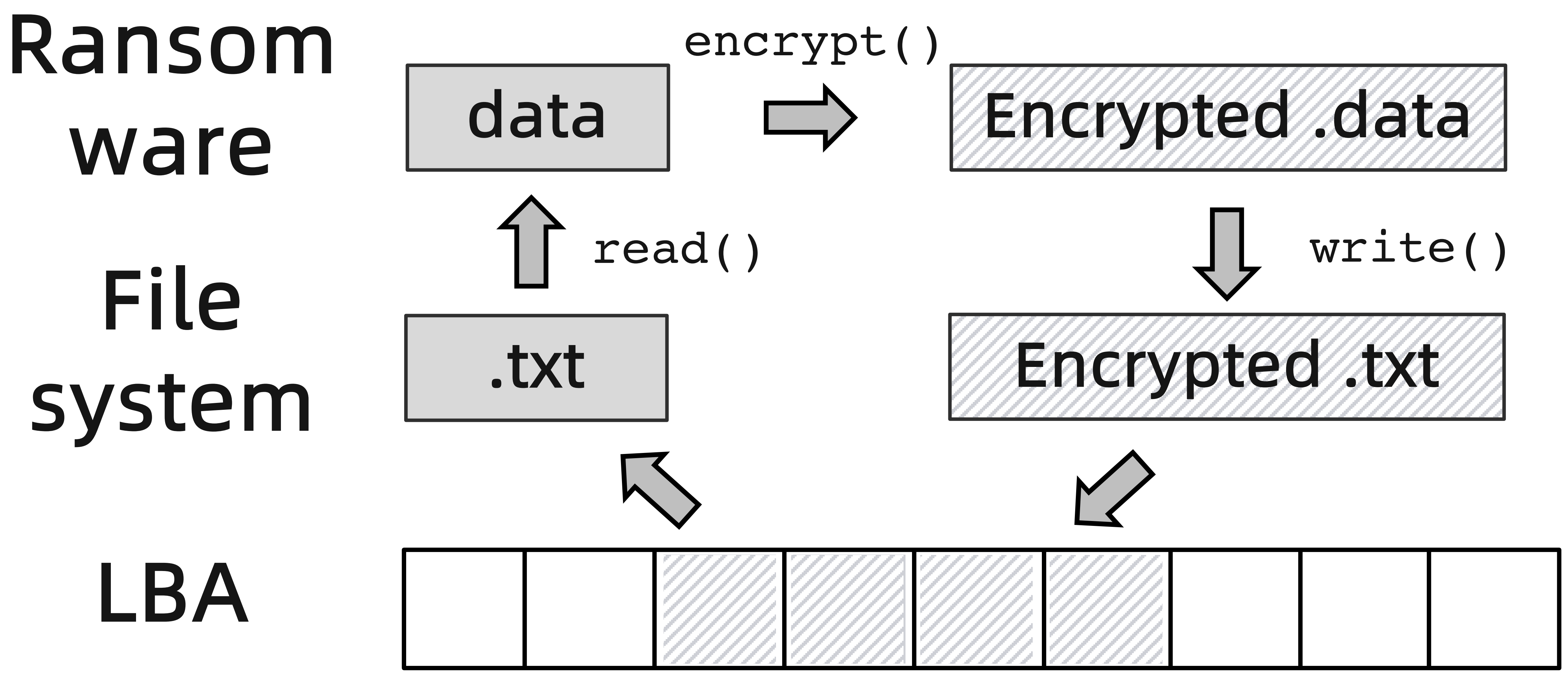
A New Hope



IO Patterns in Flash Pages

Old data NOT reclaimed immediately

Opportunity: Part I



Ransom ware

data

encrypt()

Encrypted .data

read()

write()

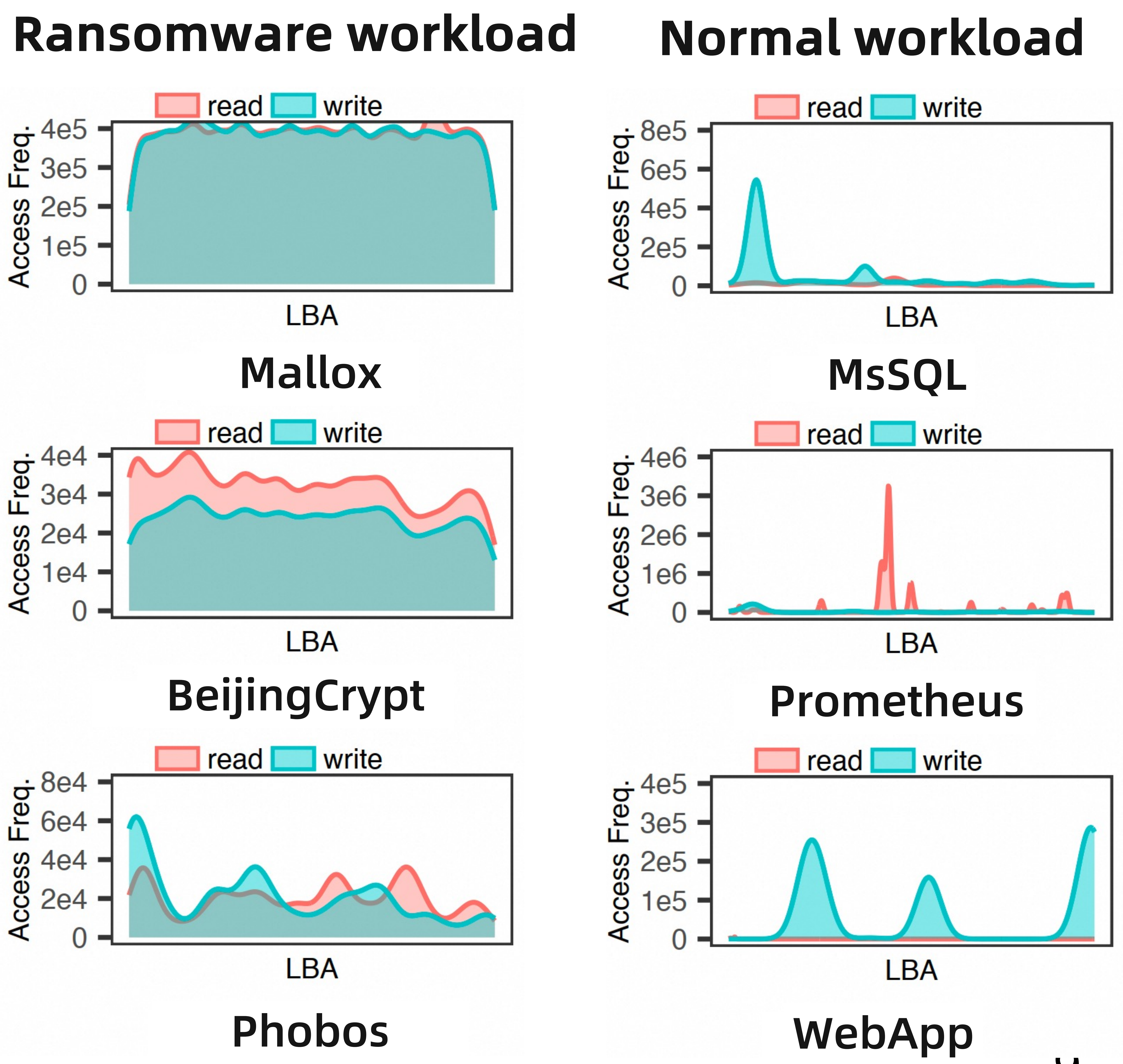
File system

.txt

Encrypted .txt

LBA

Distinct access patterns on LBA



Ransomware workload

Normal workload

Mallox

MsSQL

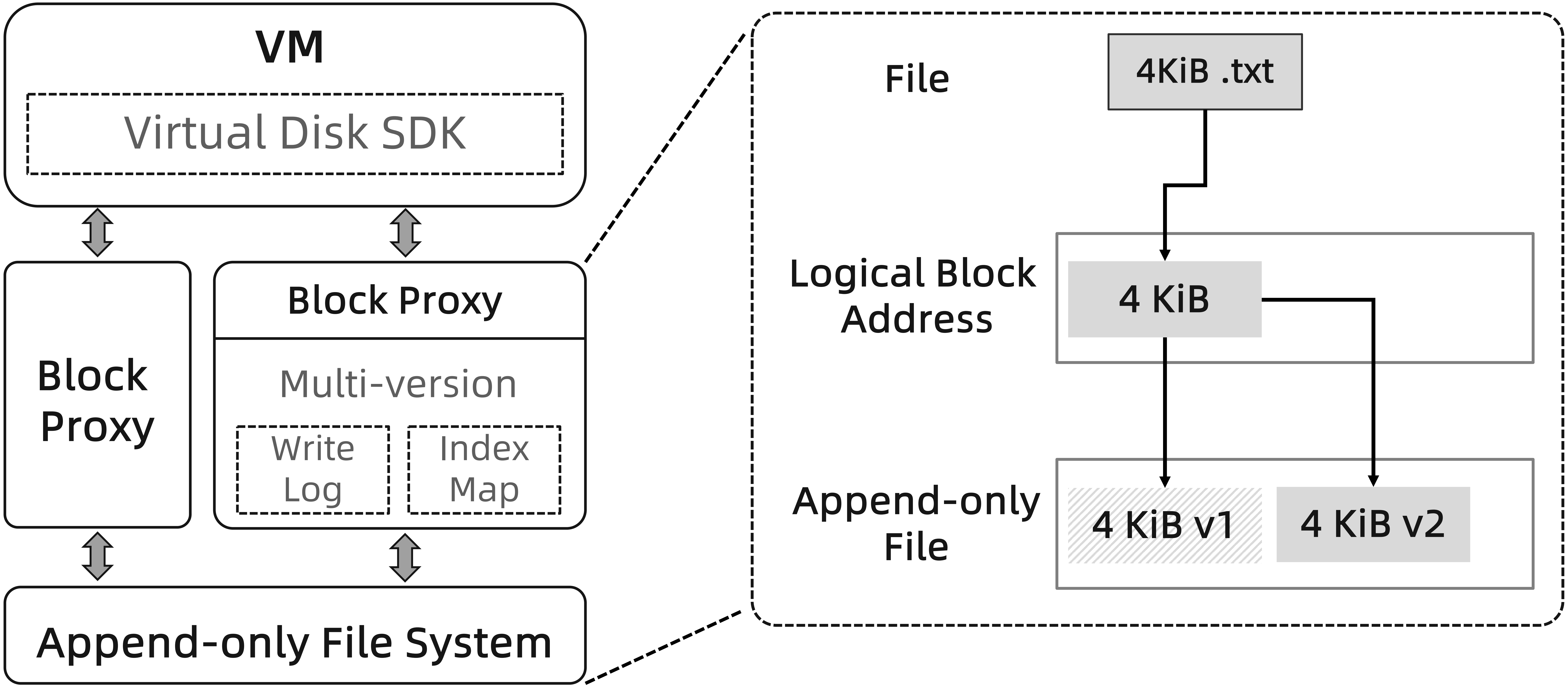
BeijingCrypt

Prometheus

Phobos

WebApp

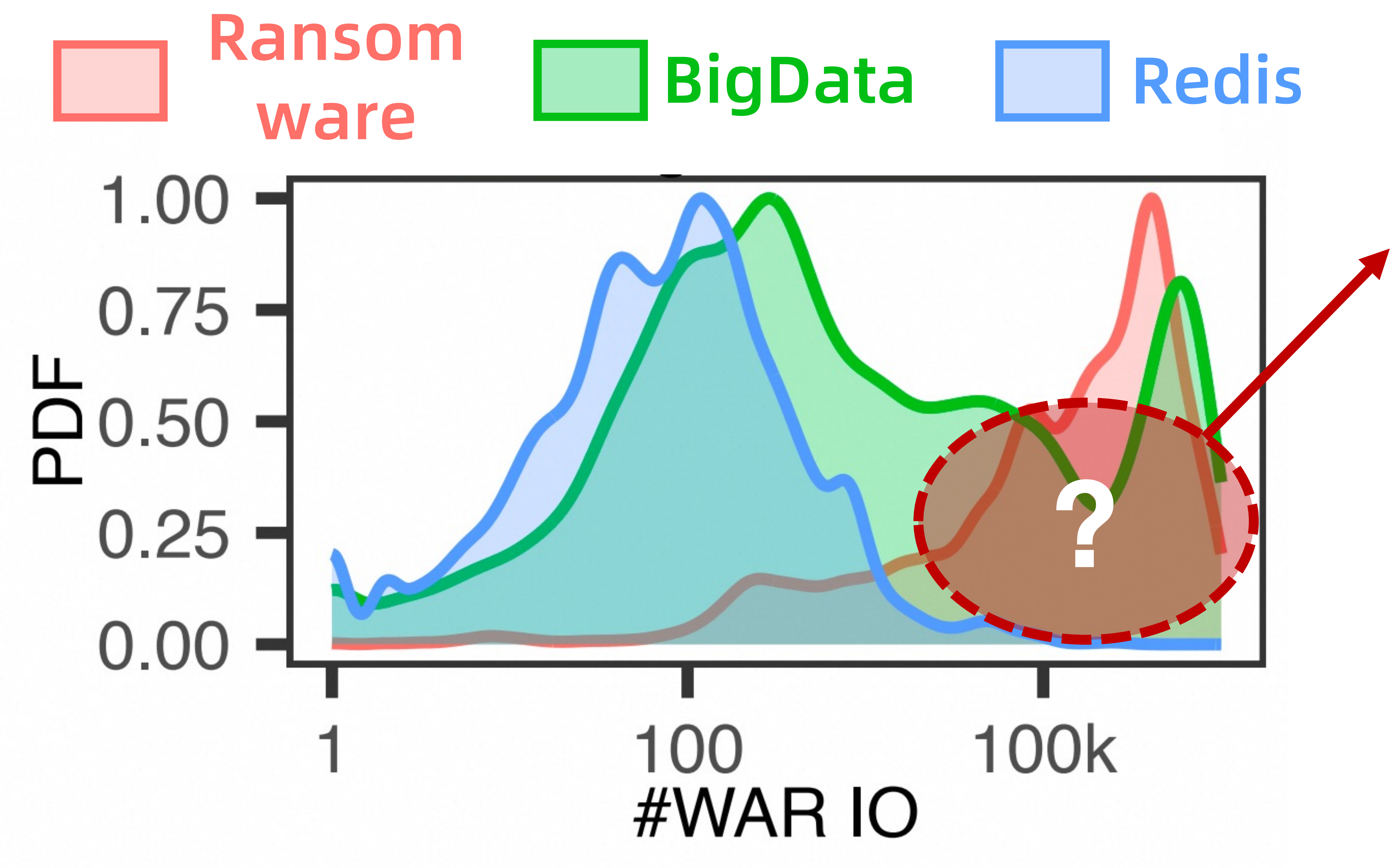
Opportunity: Part II



EBS is multi-version by nature!

Challenge 1

Count of **Write-After-Read (WAR)** IO



False positive & False negative Under Simple Features

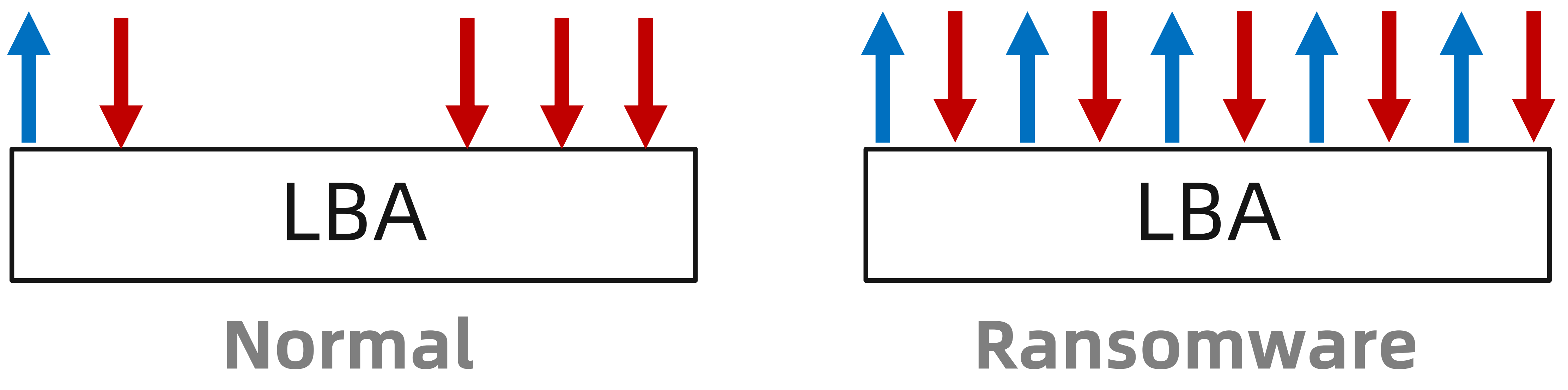
1. Limited SSD on chip resources
2. Various cloud workload

Existing features are insufficient!

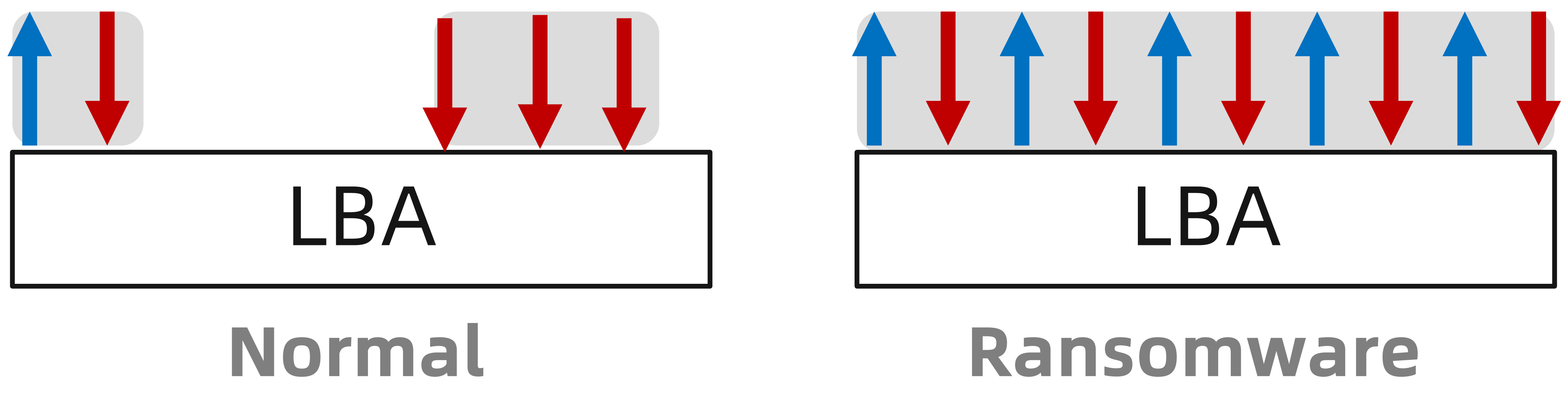
Key Tech 1: Feature Engineering

For Challenge 1

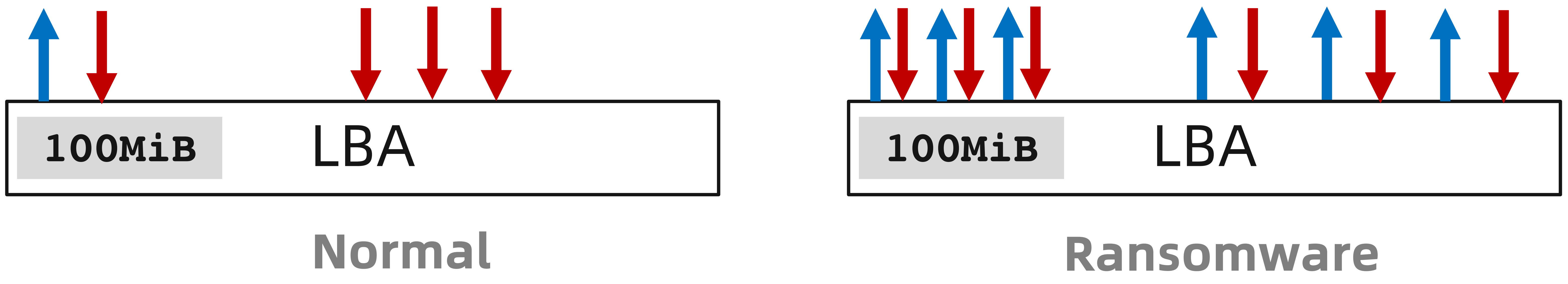
↑ read() ↓ write()



Pattern 1: Equivalent read and write



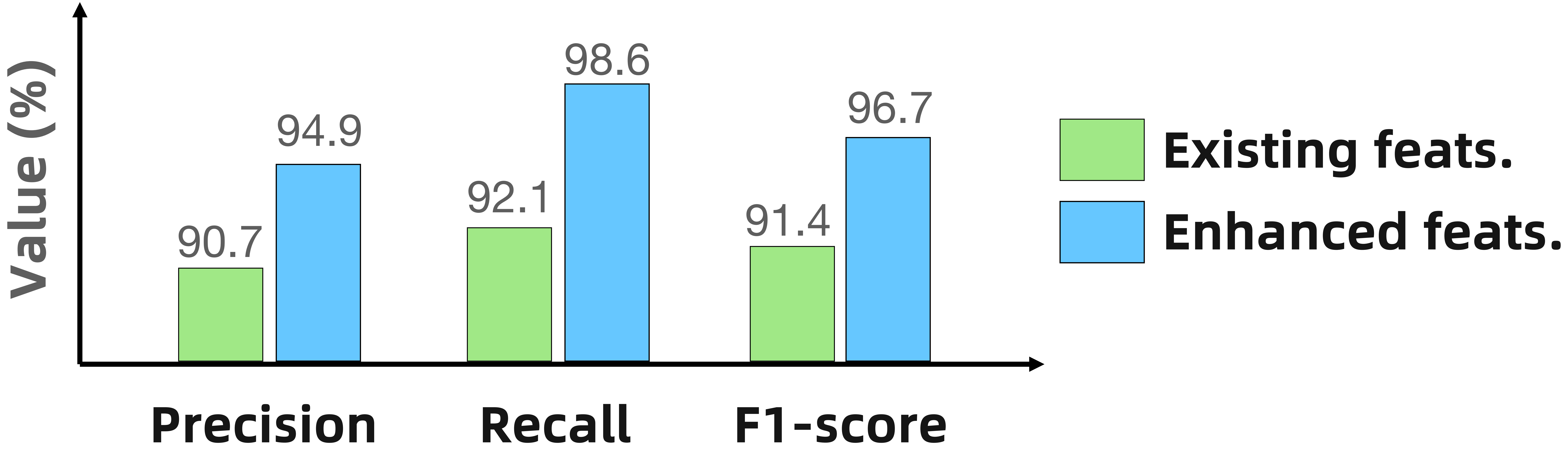
Pattern 2: Larger working set size



Pattern 3: WAR IO on the LBA head region

Three unique IO patterns from real-world ransomware trace

Challenge 2

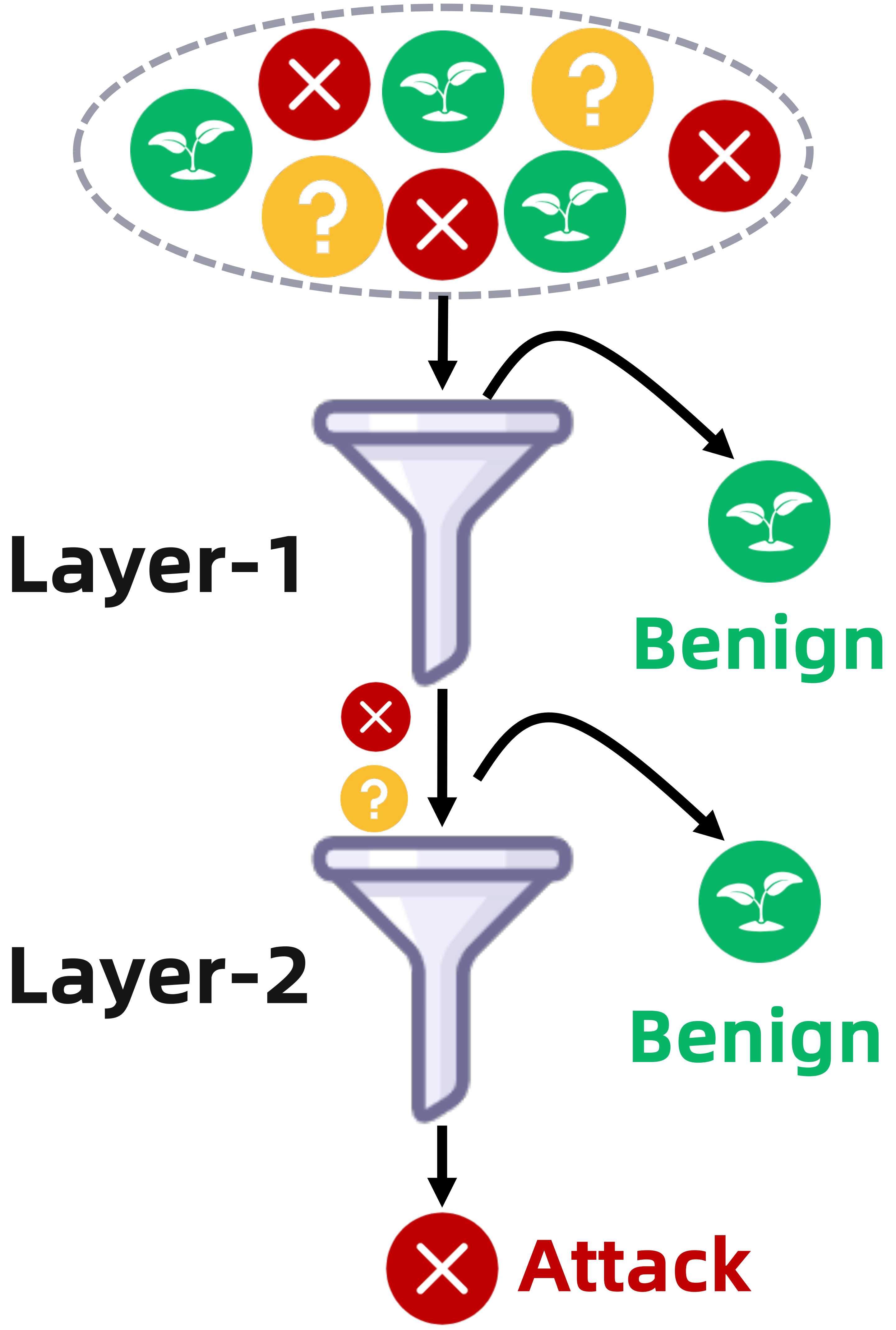


Need additional 20% machines for feature calculation

Accurate but not efficient!

Key Tech 2: Casading Two-layer Model

For Challenge 2



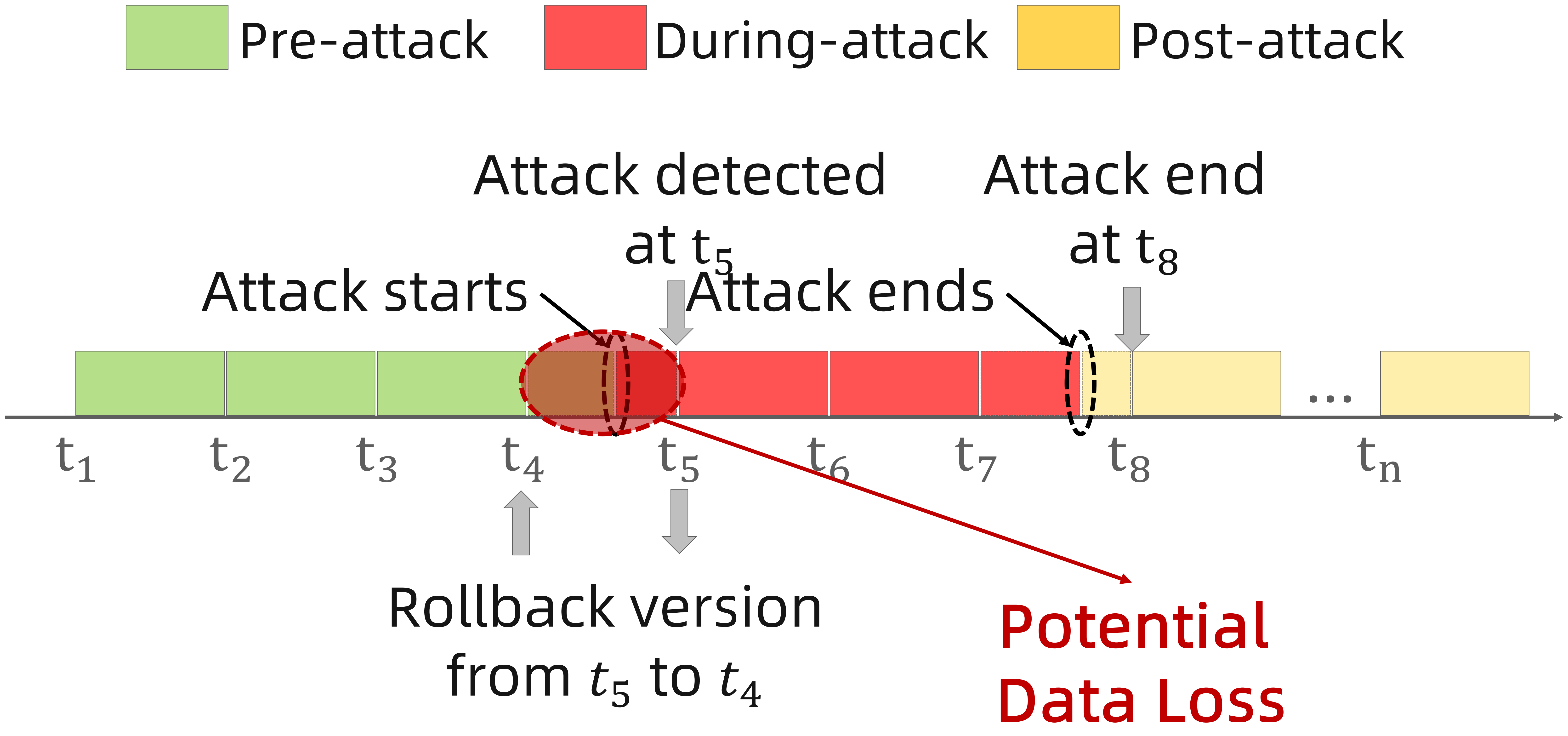
Layer-1: Fast Filtering

O(1) Features ✚ Decision Tree

Layer-2: Accurate Check

O(LogN) Features ✚ XGBoost

Challenge 3



🟩 Pre-attack 🟥 During-attack 🟨 Post-attack

Attack detected at t_5

Attack end at t_8

Attack starts

Attack ends

t_1 t_2 t_3 t_4 t_5 t_6 t_7 t_8 … t_n

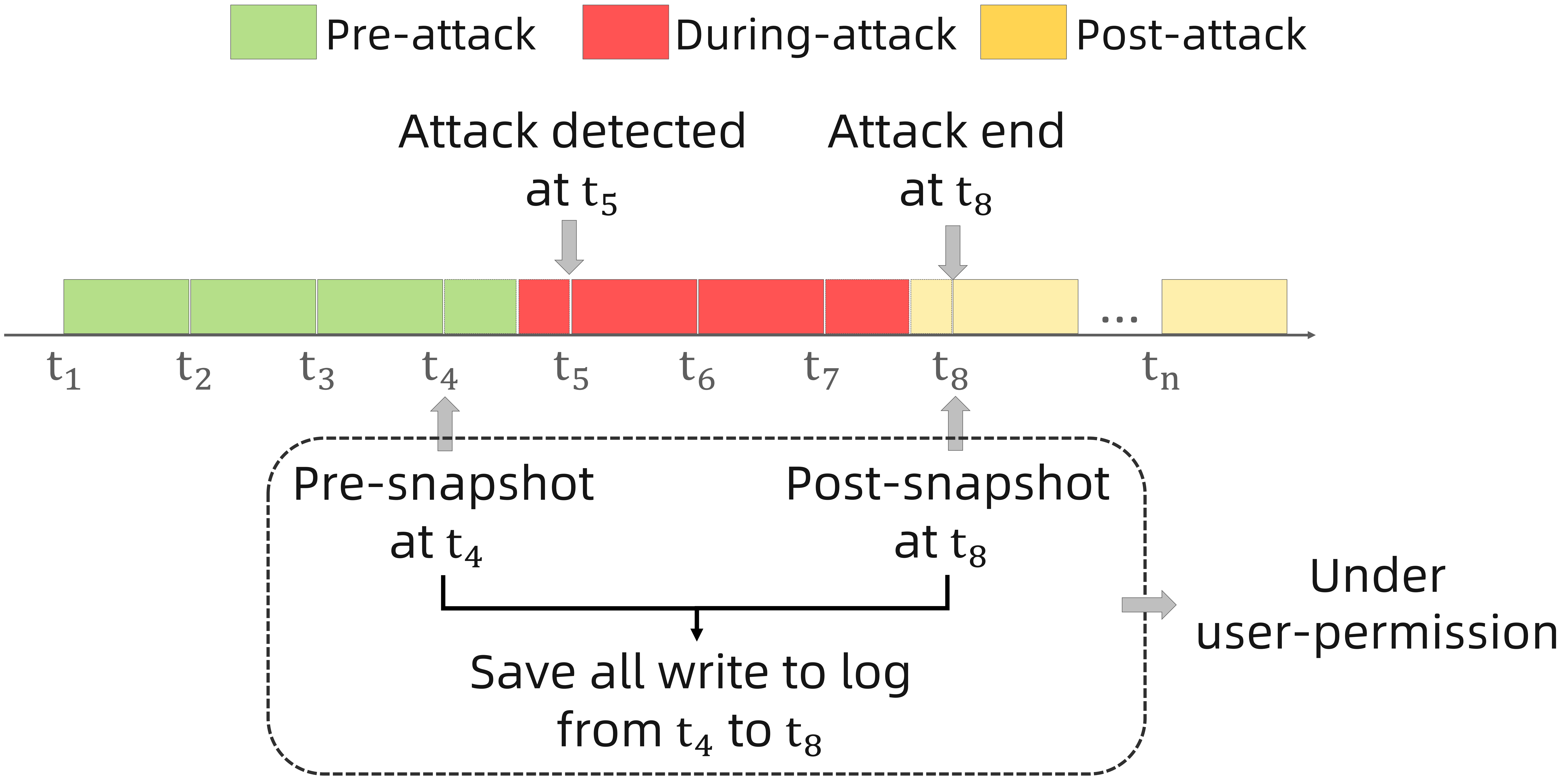
Rollback version from t_5 to t_4

Potential Data Loss

Normal IO could be lost due to direct rollback!

Key Tech 3: Data Recovery

For Challenge 3



🟩 Pre-attack 🟥 During-attack 🟨 Post-attack

Attack detected at t_5

Attack end at t_8

Pre-snapshot at t_4

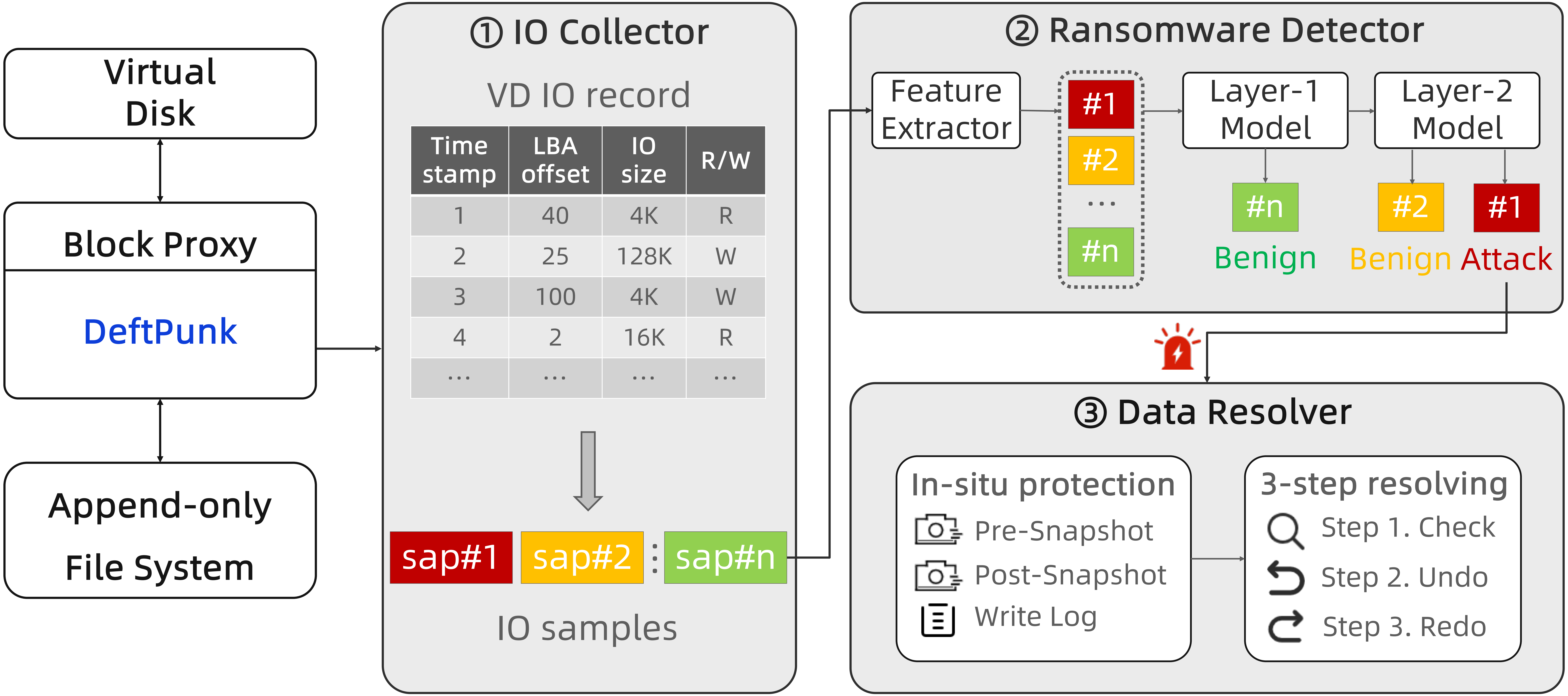
Post-snapshot at t_8

Save all write to log from t_4 to t_8

Under user-permission

Pre and post-snapshot ensure zero data loss!

DeftPunk - Put All Together



Time stamp	LBA offset	IO size	R/W
1	40	4K	R
2	25	128K	W
3	100	4K	W
4	2	16K	R
…	…	…	…

Content

01 Ransomware 101

02 Common Protections

03 DeftPunk

04 **Evaluation**

05 Discussion

Evaluation Setup

Platform

- For 30K VDs cluster
- 7 vCPUs with 2.7 GHz
- 32 GiB Memory

Normal Trace

16 types of cloud application

…

Ransomware Trace

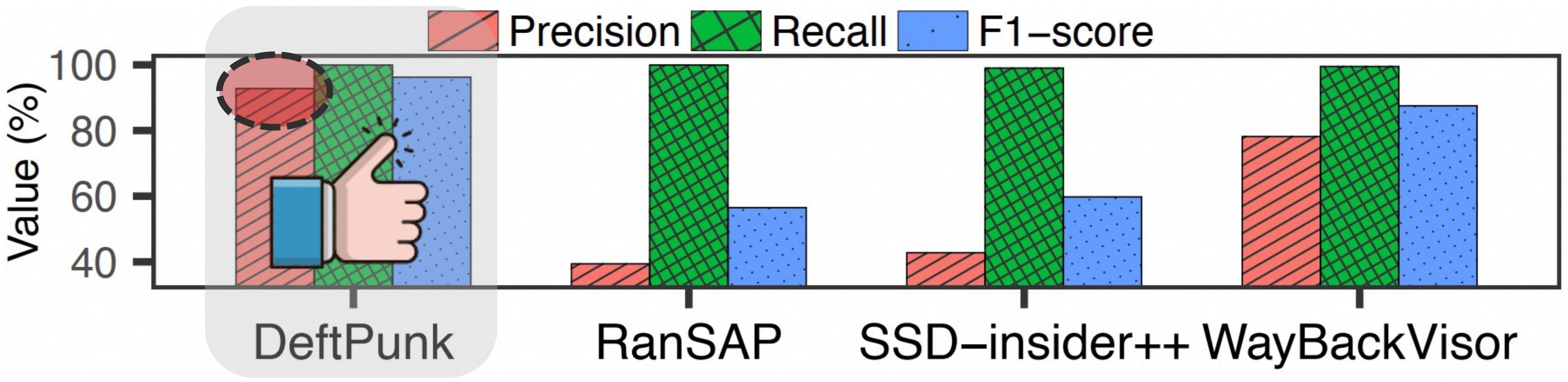
13 ransom families × 6 OSes × 5 APPs = 390 setups

loki
Sodinokibi
babuk
phobos
……

WinServer
CentOS
……

MySQL
ZIP CRYPT
Massive IO
……

Experiment Results

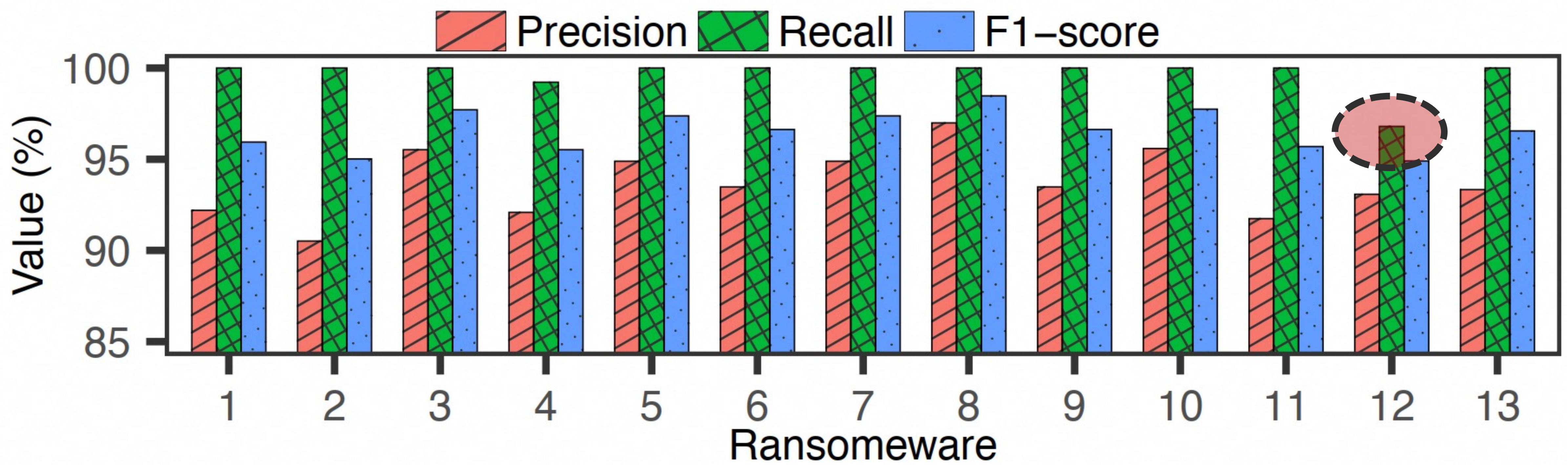


Overall performance

≈ 100% Recall and 98% Precision

False positive

- Encryption, format conversion
- Detect-notify-rollback



Zero-shot performance

Accurate detection of unseen attack

False negative

- Low recall of Babuk
- Do not encrypt txt files

More evaluations in the paper (ablation study, runtime overhead, etc)

Content

01 Ransomware 101

02 Common Protections

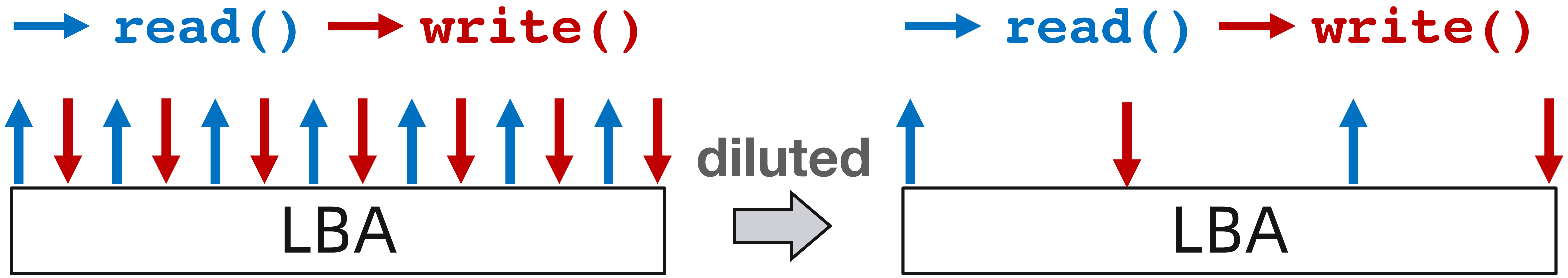
03 DeftPunk

04 Evaluation

05 **Discussion**

Call For Attention

- New Trend



WannaCry, CPU utilization < 25%, throughput <10%

- Other Attacks
  - Directly destroy data
  - Create after delete

DeftPunk dataset

https://tianchi.aliyun.com/dataset/177511

Never-ending arms race!

THANKS

Q&A

Ransom Access Memories: Achieving Practical Ransomware Protection in Cloud with DeftPunk