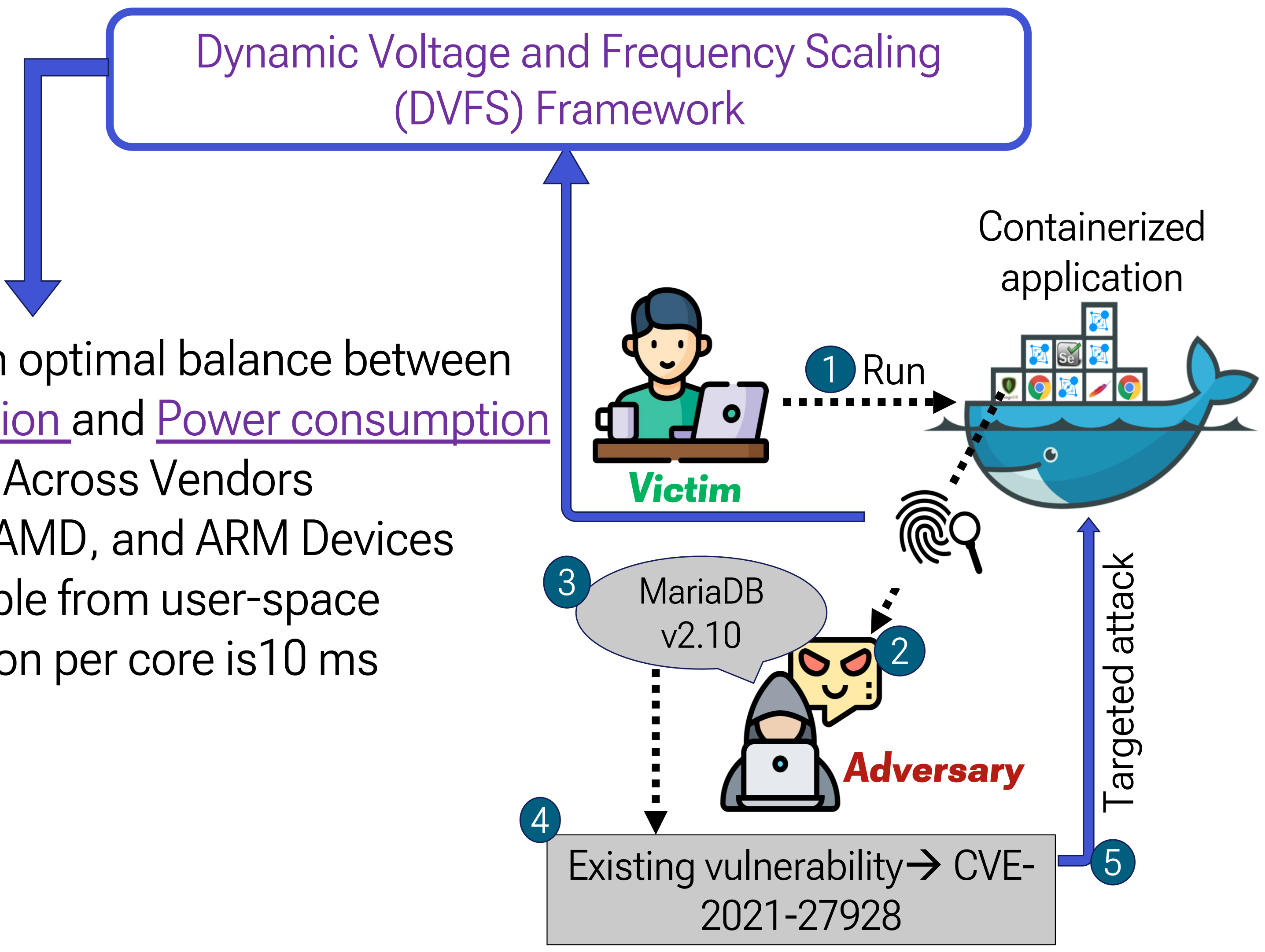
Dynamic Frequency-Based Fingerprinting Attacks against Modern Sandbox Environments

Debopriya Roy Dipta, Thore Tiemann, Berk Gulmezoglu (Faculty), Eduard Marin, Thomas Eisenbarth

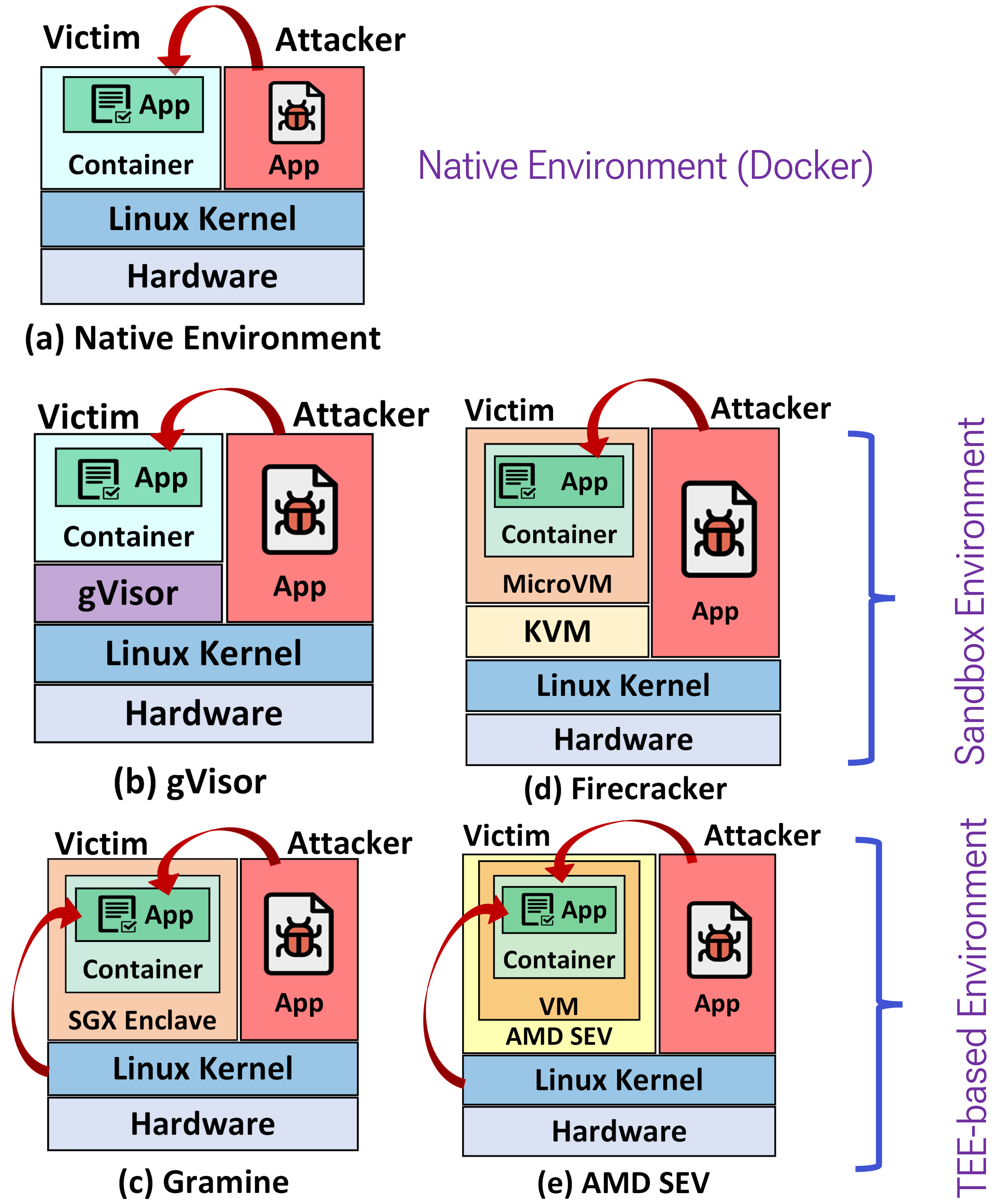
Project Statement


Dynamic Voltage and Frequency Scaling (DVFS) Framework
Containerized application
1 Run
Victim
2
3 MariaDB v2.10
Adversary
4 Existing vulnerability→ CVE-2021-27928
5
Targeted attack

- Maintain optimal balance between CPU utilization and Power consumption
- Support Across Vendors
  - ✓ Intel, AMD, and ARM Devices
- Accessible from user-space
- Resolution per core is10 ms

Hypothesis: CPU frequency information can constitute a unique application's fingerprint.

Threat Model



(a) Native Environment

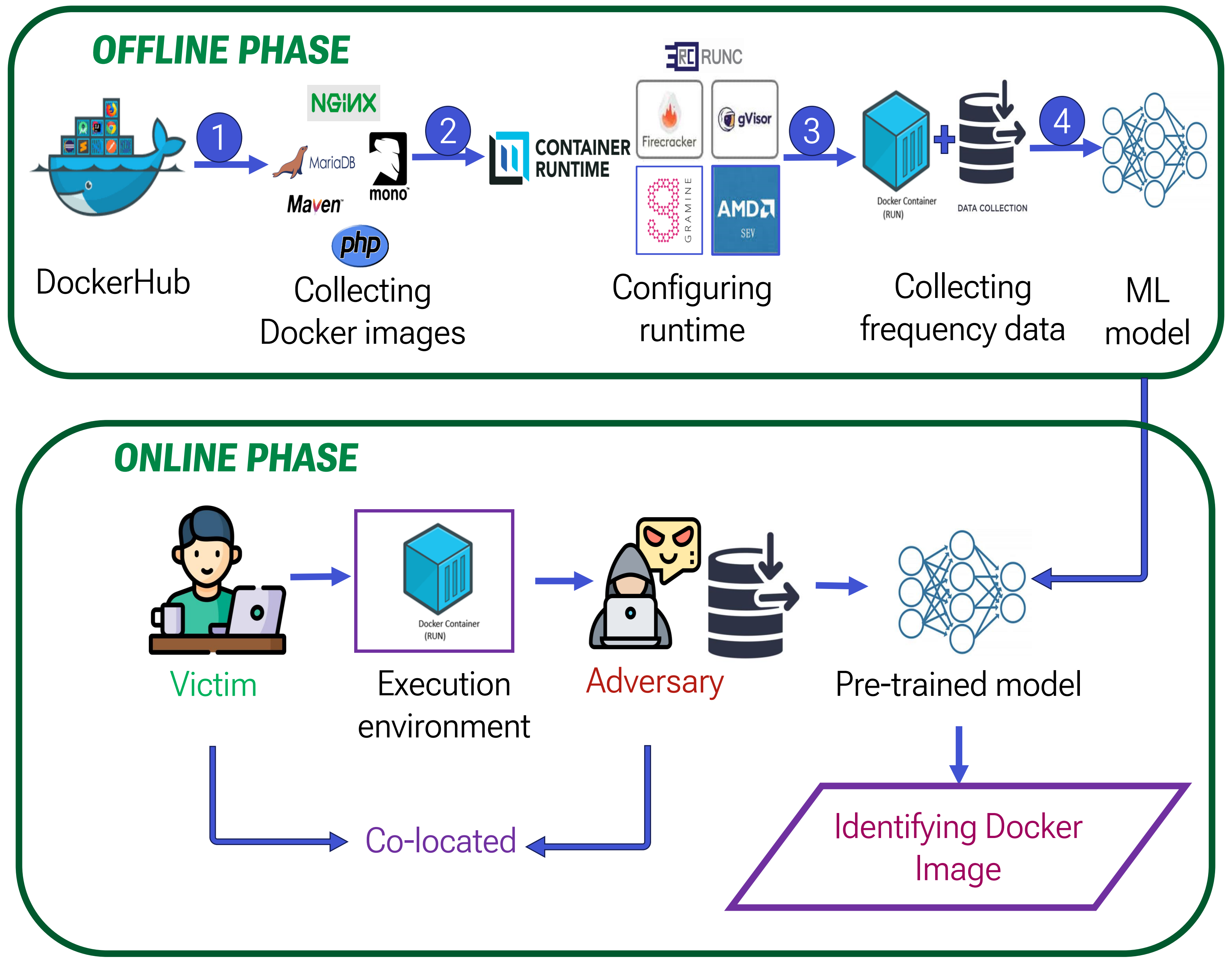
(b) gVisor

(d) Firecracker

(c) Gramine

(e) AMD SEV

Methodology



Results

Execution Environment	# of containers	Microarchitectures					
		Comet Lake	Cascade	Broadwell	Skylake	Coffee Lake	AMD EPYC
Native	126	**84.5%**	83.03%	73.37%	81.04%	74.16%	79.60%
Firecracker	126	-	**73.04%**	-	72.01%	-	-
gVisor	126	-	71.20%	**71.7%**		-	
Gramine	50	-	-	-	-	**91.4%**	-
AMD-SEV	107	-	-	-	-	-	**79.8%**

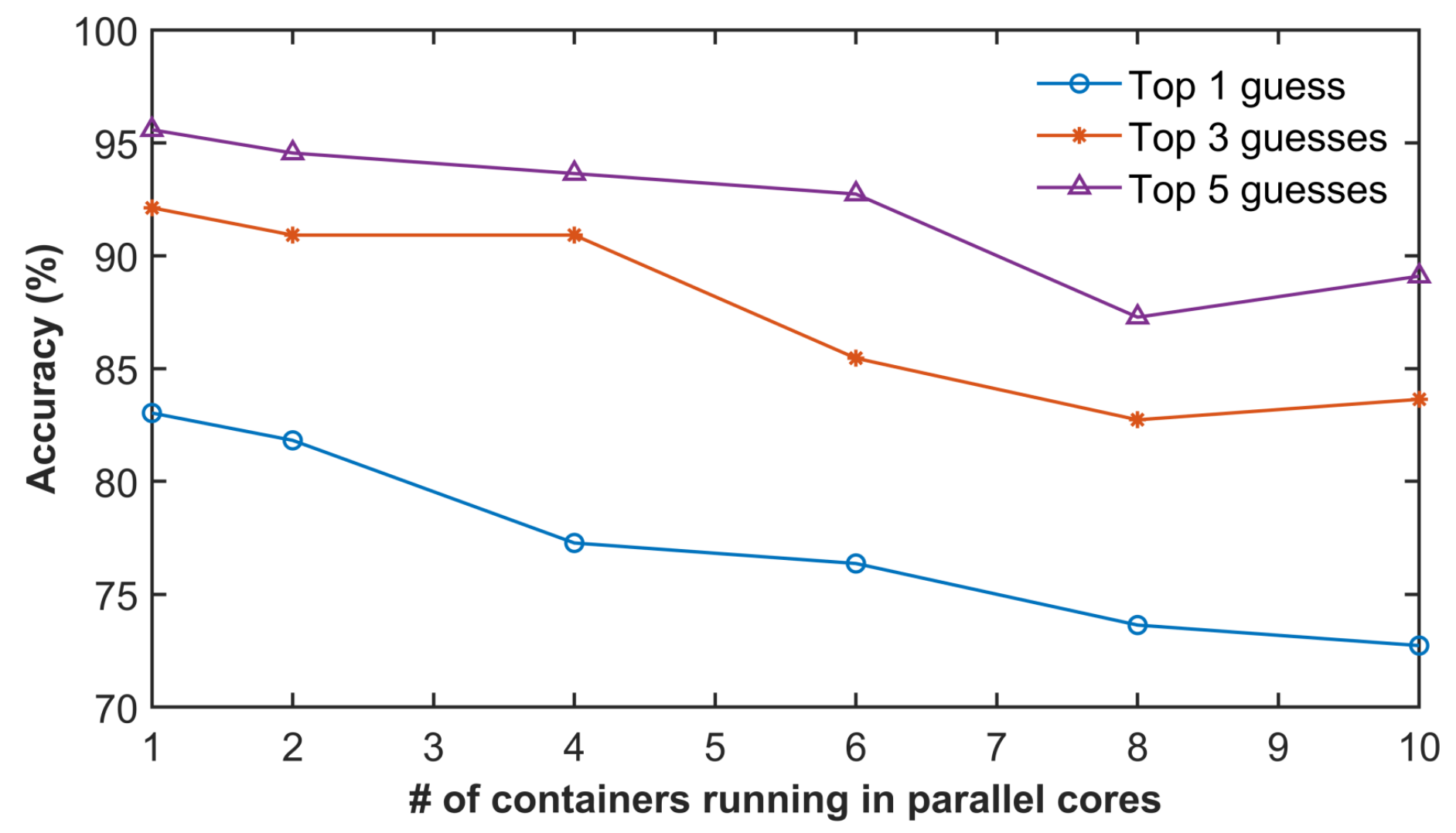
Outcome: The average accuracy over different microarchitecture and execution environment is more than 70%.

a) Evaluation: Simultaneous execution of multiple containers

- # of containers executed simultaneously: 2-10.
- Each container is pinned to separate cores.
- Hyperthreading Case: Two containers are pinned into two sibling threads

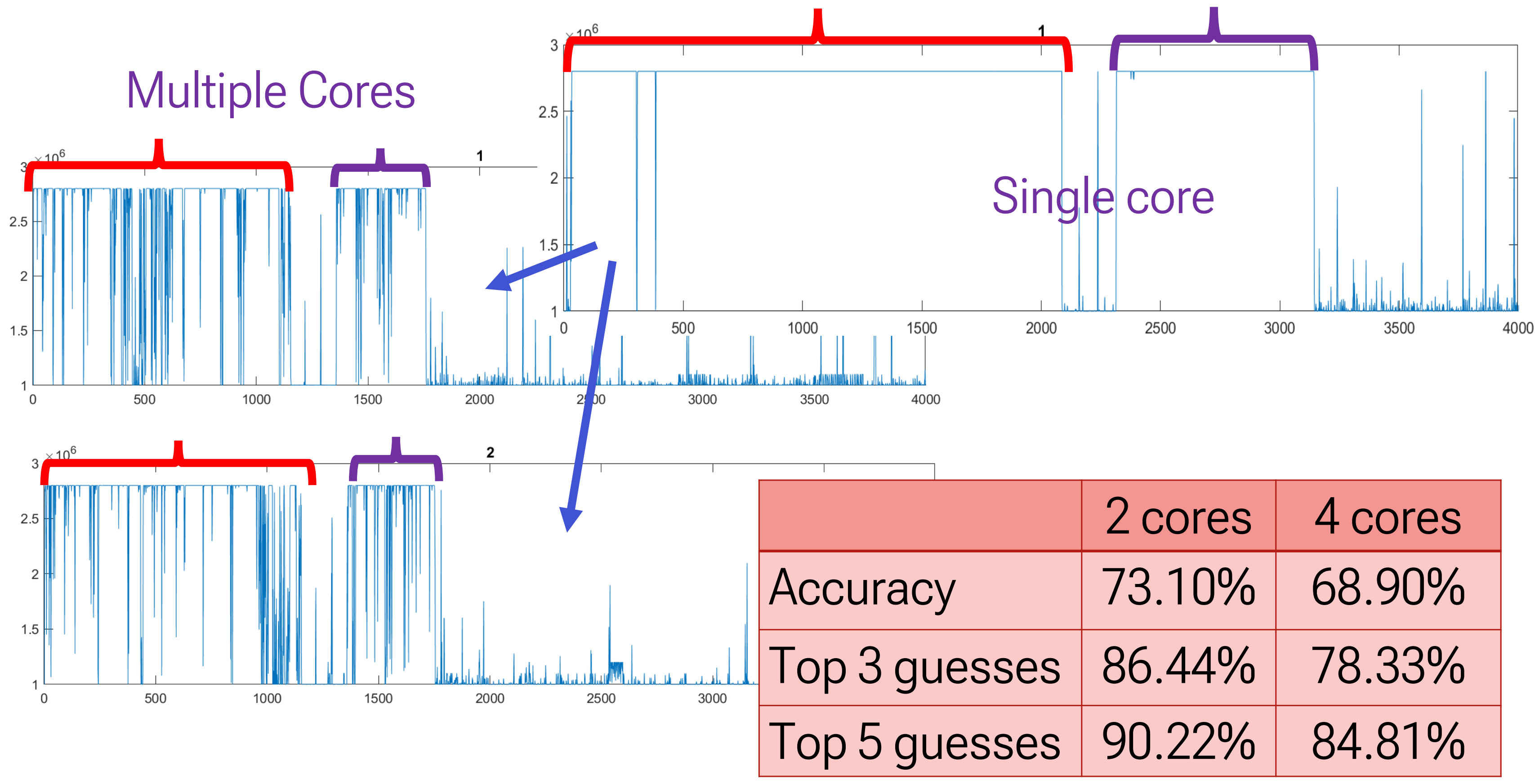
✓ On average, every container introduces ≈ **1.5%** accuracy drop

✓ ***Hyperthreading Case:*** The accuracy drops by 48.6%



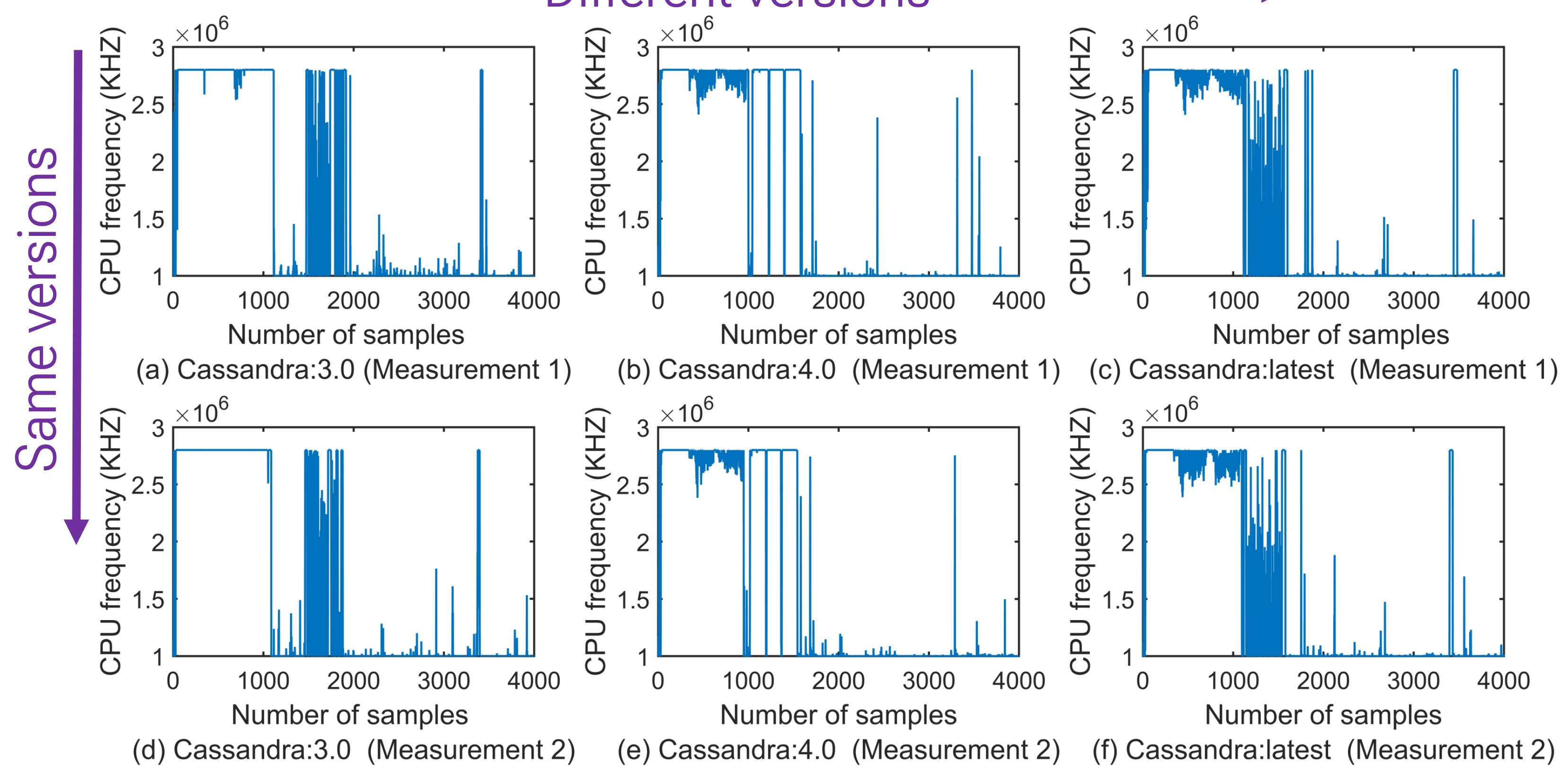
Outcome: Adversary can track multiple users or containers concurrently

b) Evaluation: Effects of assigning containers to multiple cores



	2 cores	4 cores
Accuracy	73.10%	68.90%
Top 3 guesses	86.44%	78.33%
Top 5 guesses	90.22%	84.81%

c) Evaluation: Feasibility with different versions of the Docker images



(a) Cassandra:3.0 (Measurement 1) (b) Cassandra:4.0 (Measurement 1) (c) Cassandra:latest (Measurement 1)

(d) Cassandra:3.0 (Measurement 2) (e) Cassandra:4.0 (Measurement 2) (f) Cassandra:latest (Measurement 2)

- # of Docker images: 25
- # of chosen versions/image: 5
- The acquired test accuracy: 81.02%

Outcome: Different versions of Docker images produce adequate variability in signatures to fingerprint them.

Conclusion

- Fingerprinting running containers in native, sandboxed, and TEEs.
- Success rate: more than 70% in all these environments
- Examine various scenarios that an attacker can face in cloud computing
- Countermeasures:
  - ✓ Artificial noise injection → client-based
  - ✓ Syscall pattern monitoring → cloud-based

References

[1] D. R. Dipta, T. Tiemann, B. Gulmezoglu, E. Marin and T. Eisenbarth, "Dynamic Frequency-Based Fingerprinting Attacks against Modern Sandbox Environments," 2024 IEEE 9th European Symposium on Security and Privacy (EuroS&P), Vienna, Austria, 2024, pp. 327-344, doi: 10.1109/EuroSP60621.2024.00025.

[2] Dipta, D.R. and Gulmezoglu, B., 2022, December. Df-sca: Dynamic frequency side channel attacks are practical. In Proceedings of the 38th Annual Computer Security Applications Conference (pp. 841-853).