Hide and Seek with AI

Can a device give away the model inside?

Sheikh Muhammad Farjad · PhD Candidate, College of IS&T (Advisor: Robin Gandhi)

University of Nebraska Omaha

Partially supported by

ERDC ENGINEER RESEARCH & DEVELOPMENT CENTER

US Army Corps of Engineers

01 HIDE — THE PROBLEM

AI now runs on the device itself.

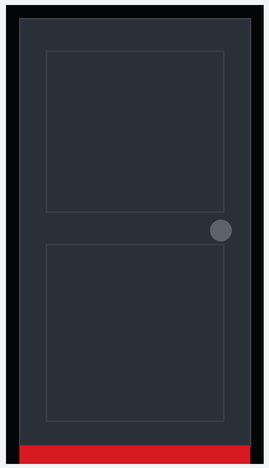


Code, weights, data:
all locked away

Hidden… right?

02 LEAK — WHAT IS KNOWN

Every run leaves footsteps: a side channel



the model

How long each step takes



How the processor is used



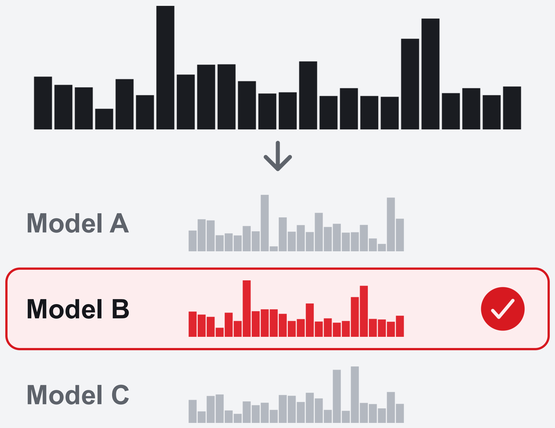
How the operating system reacts



03 SEEK — THE GAP

Can footsteps name the model on edge devices?

? device trace (illustrative)



HYPOTHESIS & APPROACH

Each model leaves its own lasting fingerprint.

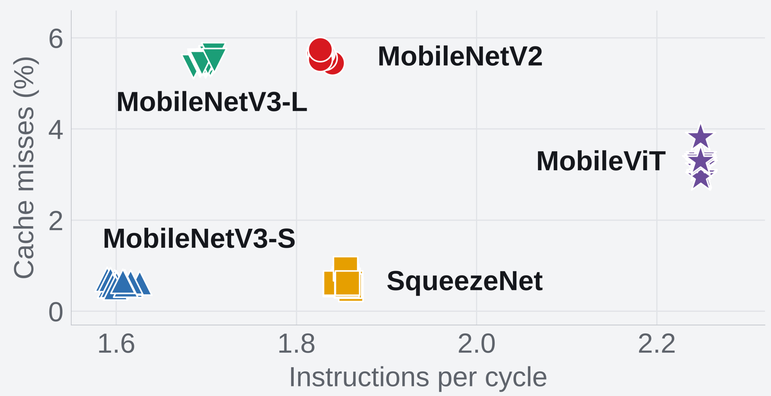
I test it across:

- TVM
- IREE
- ONNX Runtime
- system load

KEY RESULT

Preliminary · lab server

5 models → 5 distinct fingerprints



KEY INSIGHT

Locking the code
≠
Hiding the model

Why it matters: revealing the model exposes proprietary AI.

Impact: knowing what leaks shows how to protect it.

WHAT IS NEXT

Confirm on real edge devices, across frameworks and system load

Let's talk: edge devices, real-world models, collaborators

sfarjad@unomaha.edu | **Scan for my website →**