GraphMemShield

Auditing Cross-Session Leakage in Graph Memories

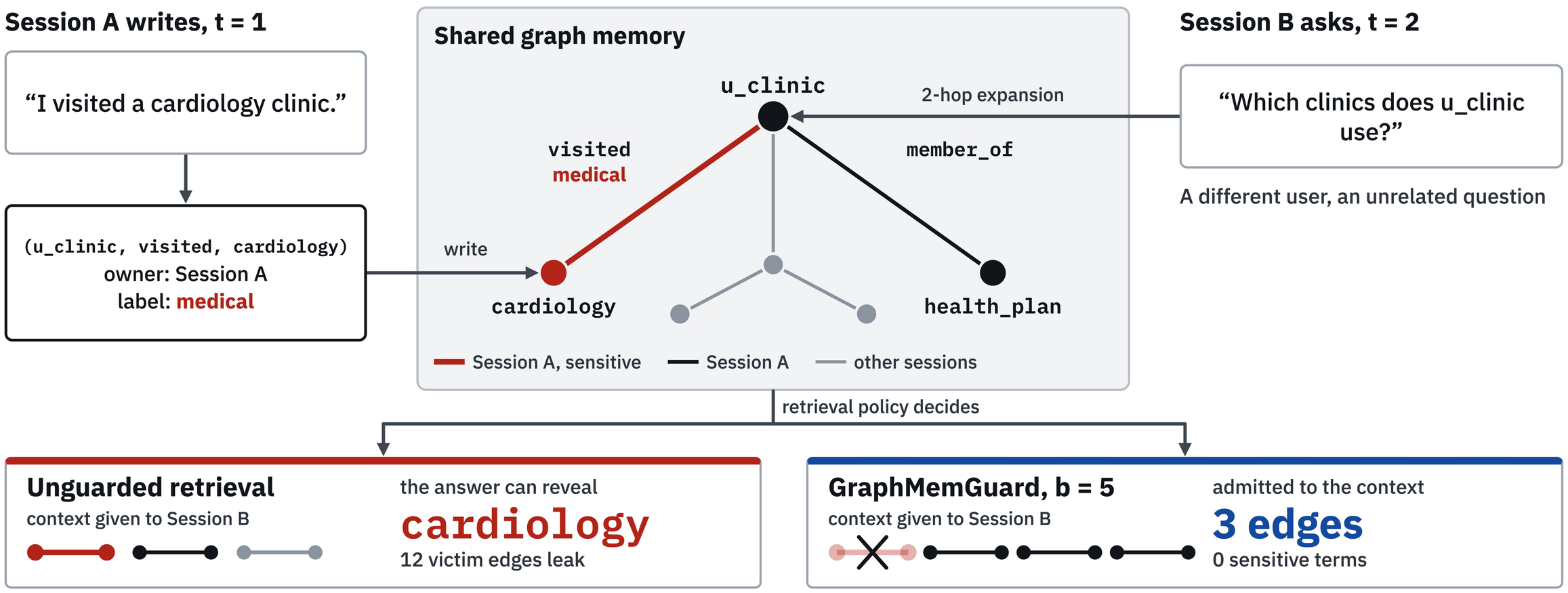
Phat T. Tran-Truong[1*], Xuan-Bach Le[1*], Son Ha Xuan[2†]

[1]Ho Chi Minh City University of Technology (HCMUT), VNU-HCM, Vietnam
[2]Digital Economy, The Business School, SGS Campus, RMIT, Vietnam
[*]Equal contribution [†]Corresponding author phatttt@hcmut.edu.vn lexuanbach@hcmut.edu.vn ha.son@rmit.edu.vn

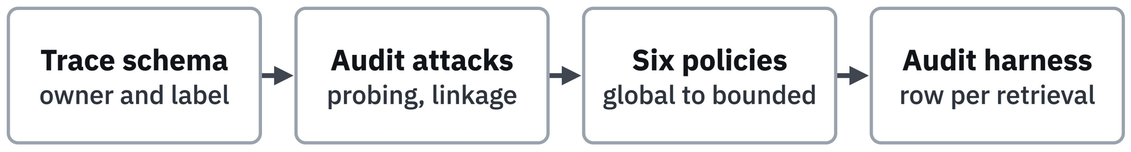
CIKM 2026
Rome, Italy

Read the paper

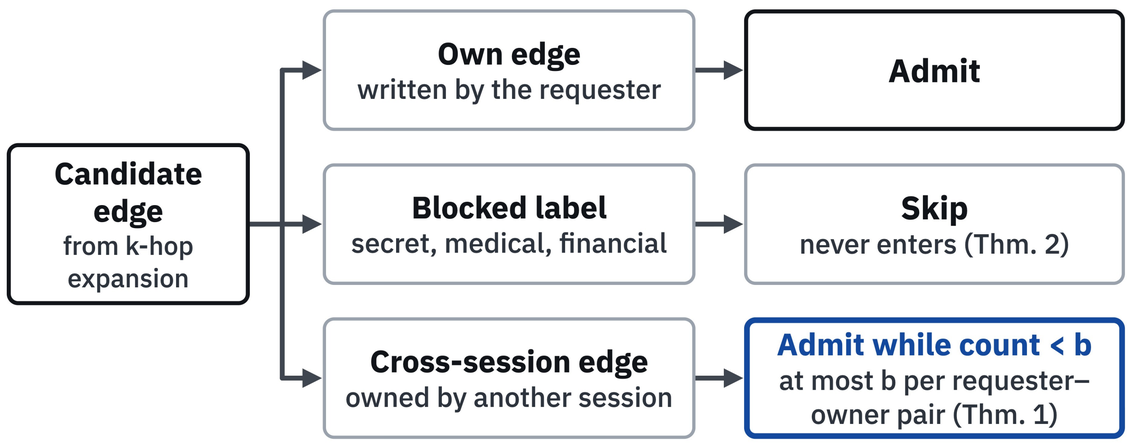
A shared graph memory can pass one user's private fact to another user



One audit suite for graph memory

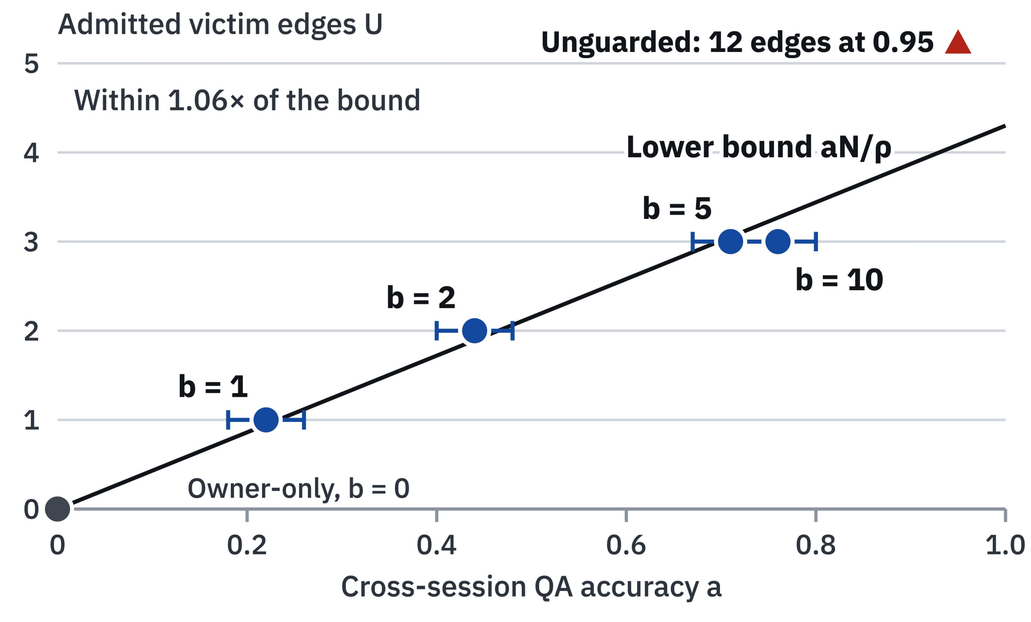


GraphMemGuard: three rules per edge

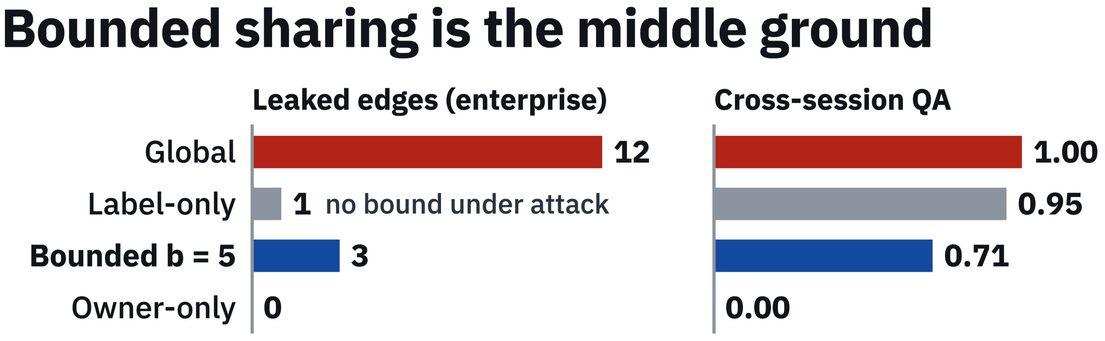


Bounded sharing sits on the frontier

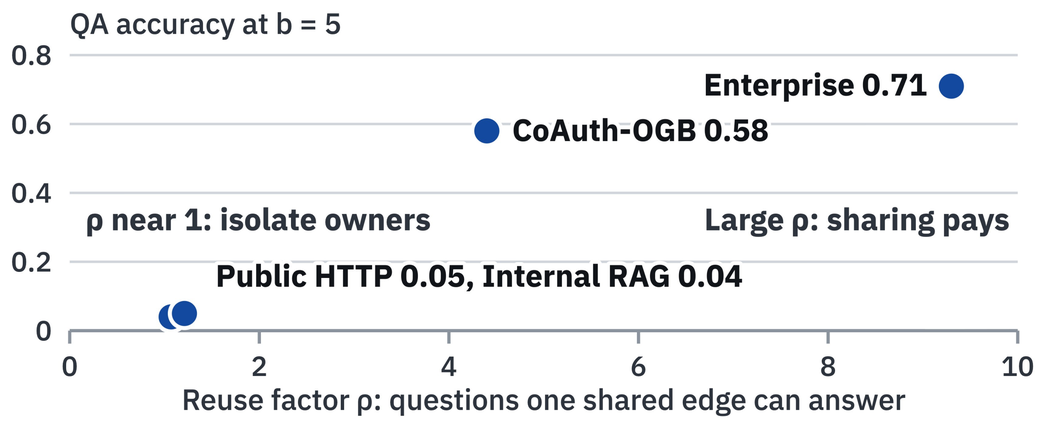
Enterprise, 10 seeds. Accuracy a needs at least aN/ρ edges (Thm. 4).



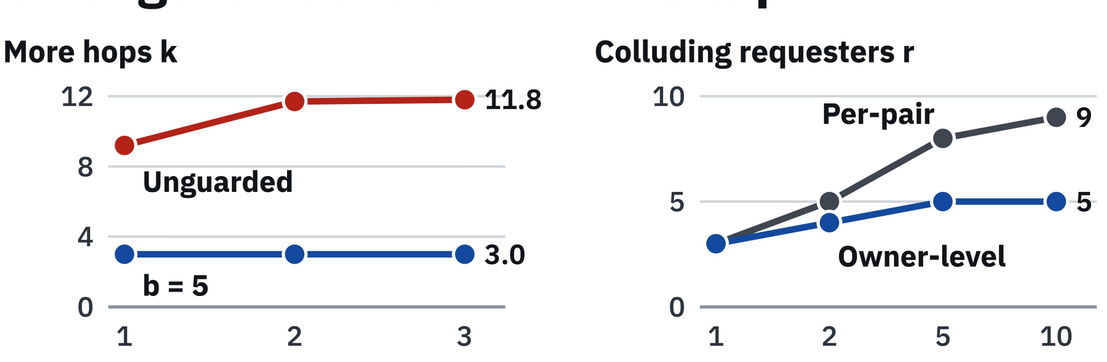
Bounded sharing is the middle ground



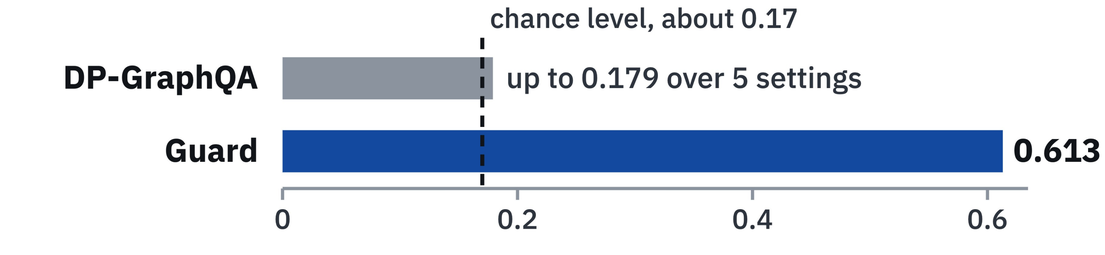
ρ tells you which policy to deploy



Stronger attacks still hit the cap



Answer-level DP stays near chance



Operator guidance

Bound exposure before the context is built.

ρ near 1: isolate. Large ρ: share with b = 5.

Add DP-GraphQA only if you can pay the margin cost.

Scope: not user-level DP; labels must be correct upstream.

dl.acm.org/doi/10.1145/3799682.3840995