KV-Auditor: Auditing Local Differential Privacy for Correlated Key–Value Estimation

CIKM 2025

Jingnan Xu[1], Leixia Wang[2], Xiaofeng Meng[1*]

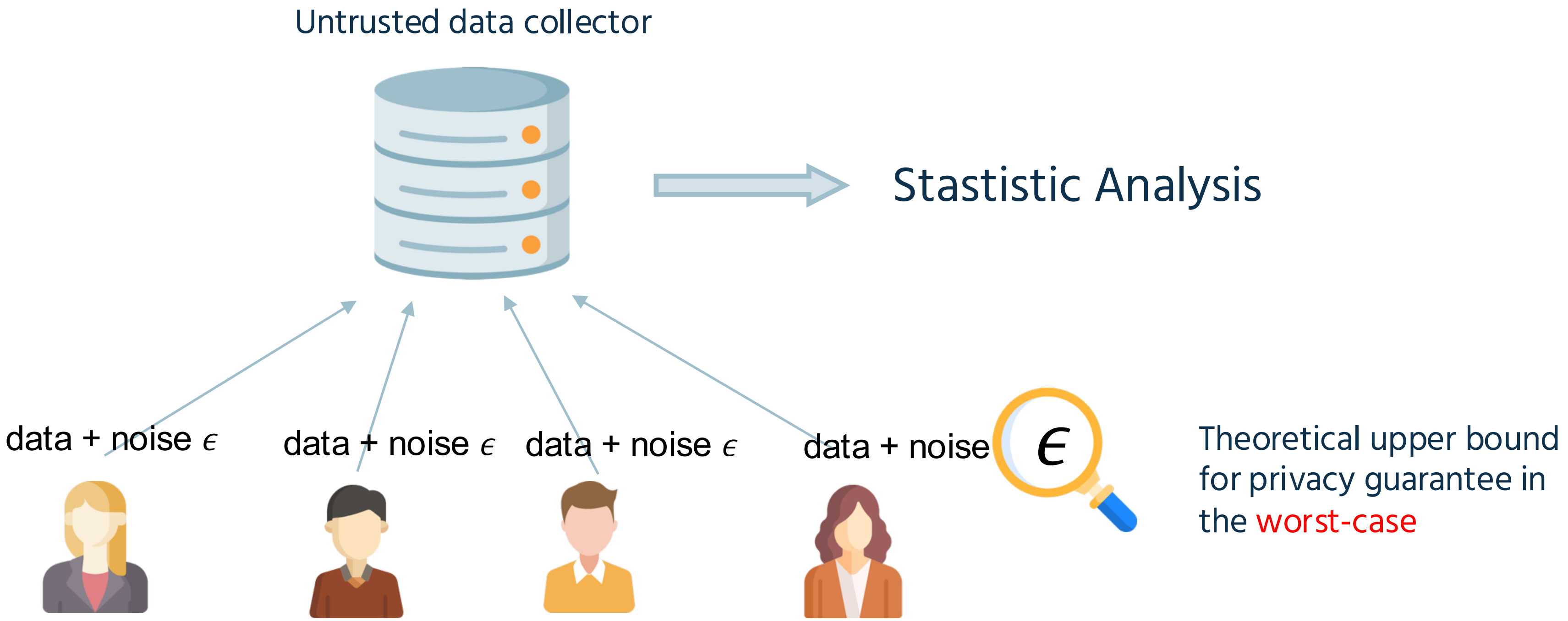
[1] Renmin University of China

[2] Northeastern University

Privacy Challenges in Data Collection

User data collection introduces privacy risks

Local Differential Privacy (LDP)



[1]Wang, Tianhao, et al. "Locally differentially private protocols for frequency estimation." 26th USENIX security symposium (USENIX Security 17). 2017.

Limitations of Theoretical ε

Algorithm Designers

- Proof/Implementation errors
- Overly loose bound

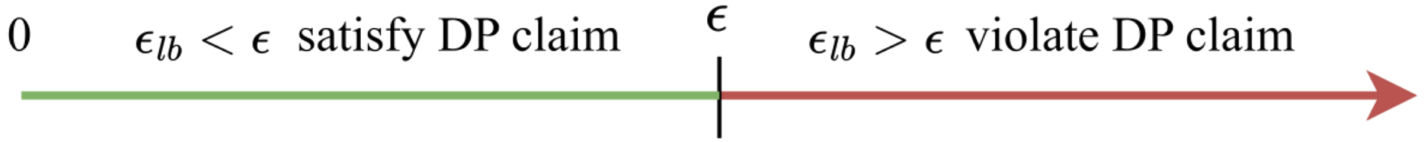
ϵ-LDP

$\epsilon = 0.5$?

Users

- Hard to undertand

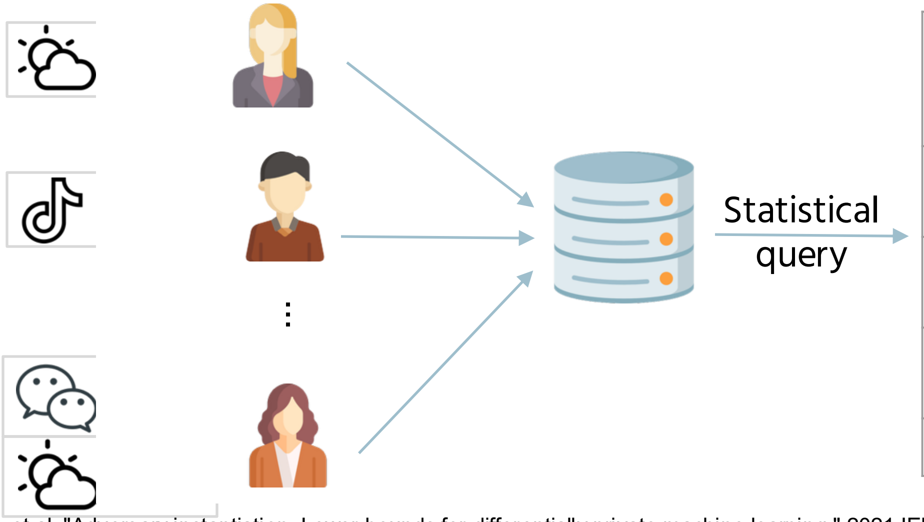
Privacy Auditing for Differential Privacy



Privacy Auditing for Differential Privacy

- ✅ Auditing under Centralized Setting
- ✅ Auditing LDP protocols for discrete data (frequency estimation)
- ❌ Auditing LDP protocols for key-value data

Challenges:
- *Continuous values → cannot be enumerated*
- *Key–value correlation*



APP	Frequency (Discrete)
	2
	1
	1

[1] Nasr, Milad, et al. "Adversary instantiation: Lower bounds for differentially private machine learning." 2021 IEEE Symposium on security and privacy (SP). IEEE, 2021.
[2] Maddock, Samuel, Alexandre Sablayrolles, and Pierre Stock. "Canife: Crafting canaries for empirical privacy measurement in federated learning." arXiv preprint arXiv:2210.02912 (2022).

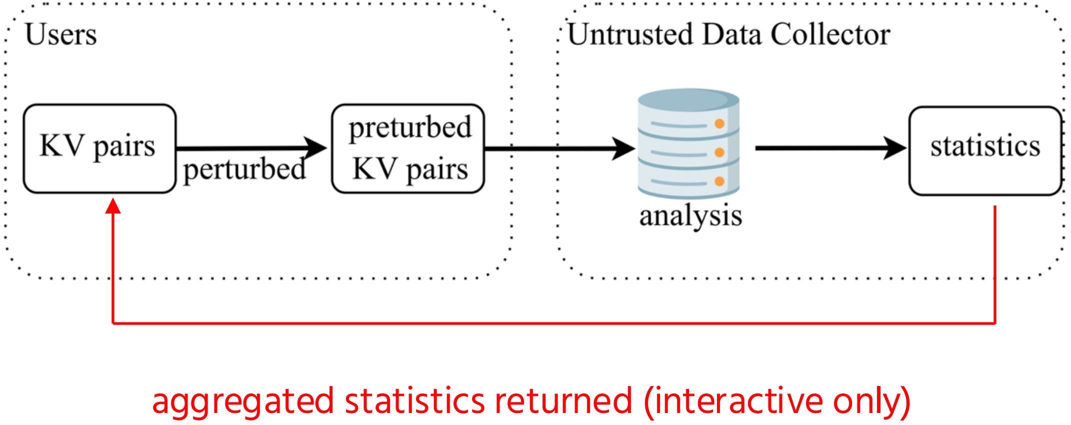
LDP Protocols for Correlated Key-Value Estimation

Interactive protocols

- PrivKVM -- multi-round estimation
- PrivKVM* -- multi-bucket extension

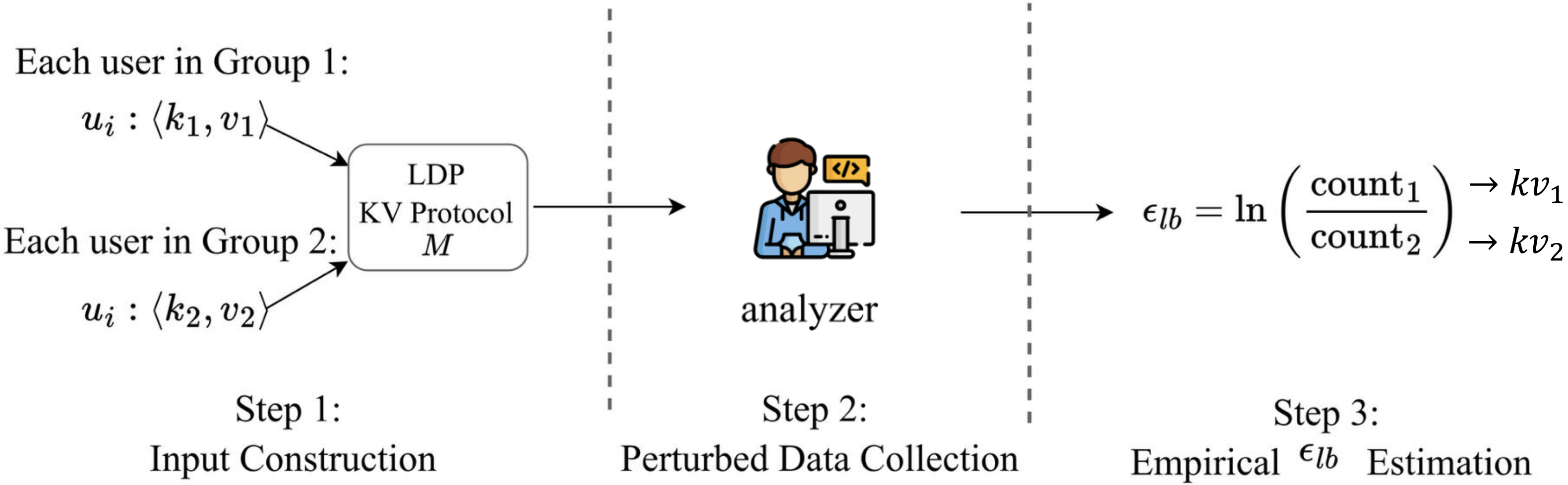
Non-interactive protocols

- PCKV -- one-shot perturbation with padding & sampling



[1] Ye, Qingqing, et al. "PrivKV: Key-value data collection with local differential privacy." 2019 IEEE Symposium on Security and Privacy (SP). IEEE, 2019.
[2] Ye, Qingqing, et al. "PrivKVM*: Revisiting key-value statistics estimation with local differential privacy." IEEE Transactions on Dependable and Secure Computing 20.1 (2021): 17-35.
[3] Gu, Xiaolan, et al. "{PCKV}: Locally differentially private correlated {Key-Value} data collection with optimized utility." 29th USENIX security symposium (USENIX security 20). 2020.

Workflow of KV-Auditor



CPP-UE/CPP-GRR: $kv_1 =< k, 1 >, kv_1 =< k, -1 >$
PCKV-UE/PCKV-GRR: $kv_1 =< k_1, 1 >, kv_1 =< k_2, -1 >$
$k_1 \neq k_2$

Calculate with the intersection of the perturbed data

KV-Auditor for Non-interactive Protocols

- **KV-Auditor for Non-interactive Protocols Perturbed data keeps a key–value structure; format depends on the mechanism.**

  UE: perturbed key + perturbed vector (e.g., PCKV-UE, CPP-UE). 

$\rightarrow < k = 1, v = [1, 0, 0, 0]>$

  GRR: perturbed key + perturbed integer (e.g., PCKV-GRR, CPP-GRR). 

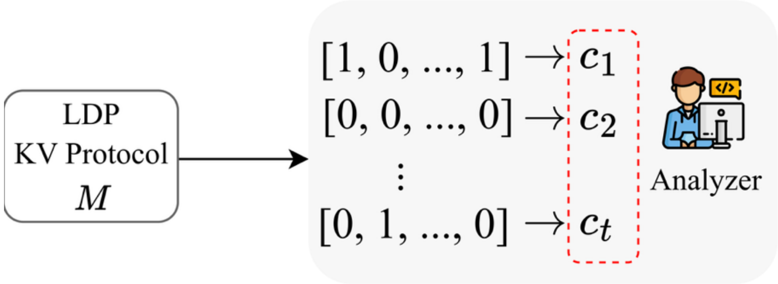
$\rightarrow <k = 1, v = -1>$

- **We design two auditors: Horizontal KV-Auditor (HKV-Auditor) and Vertical KV-Auditor (VKV-Auditor) to estimate the empirical lower bound.**

KV-Auditor for Non-interactive Protocols

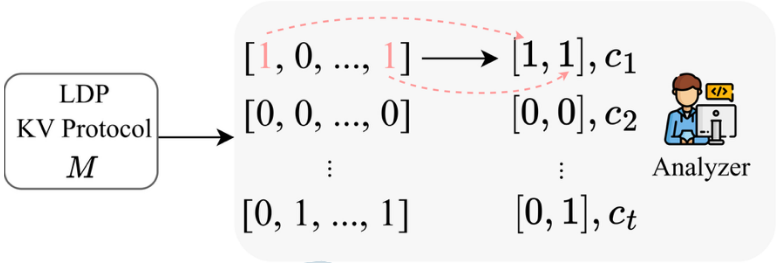
HKV-Auditor

Treats the perturbed record as a unit



- ✅ Provides tighter ϵ_{lb}
- ❌ Requires more than 10^8 users when the bit length b is large.

VKV-Auditor



Collects two bits from each perturbed vector

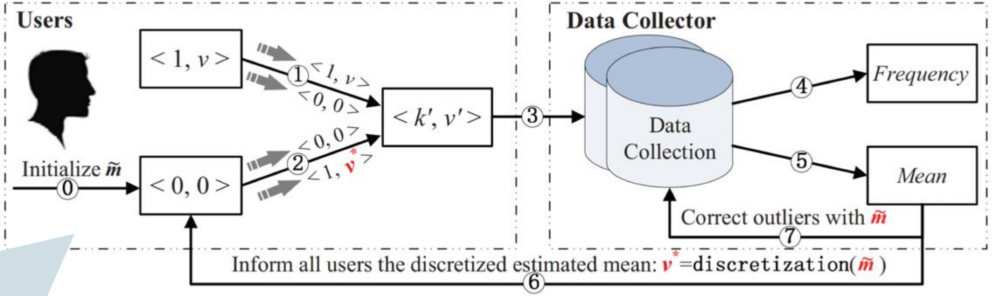
- ✅ Has shorter auditing time.
- ❌ Ignores bit dependencies.

Challenges of KV-Auditor for Interactive Protocols

- *Does the increment of privacy leakage diminish as the number of iterations increases?*
- *What is the underlying reason for the deceleration in the rate of privacy loss increment?*
- *Can the theoretical upper bound of the allocated budget for each iteration be further tightened?*

Auditing with KV-Auditor

In auditing, user data fixed→constant privacy leakage



In auditing, mean changes until stable→changing privacy leakage

Stage 1: Distribution Collection

- Perturb each user 10 times, assume all possess KV pair.
- The perturbed distribution is the average over 10 runs

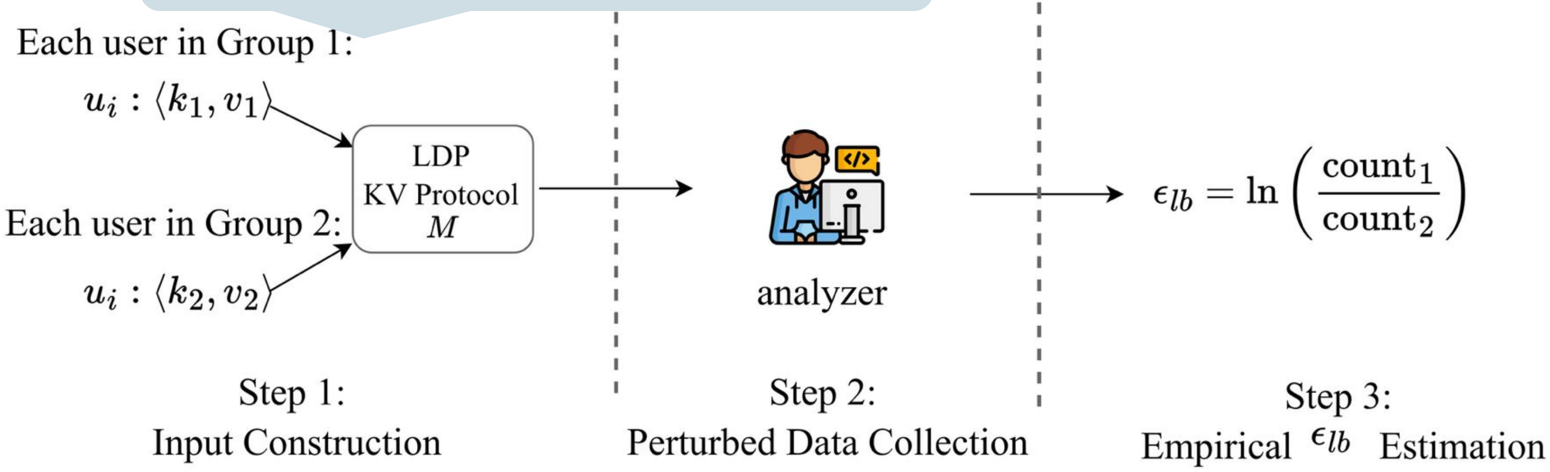
Stage 2: Distribution Separation

- Perturb once across 10 iterations
- Analyzer separates the mean-perturbed distribution (scaling applied)

[1] Ye, Qingqing, et al. "PrivKVM*: Revisiting key-value statistics estimation with local differential privacy." IEEE Transactions on Dependable and Secure Computing 20.1 (2021): 17-35.

KV-Auditor with Segmentation

Perturbation group: users are divided into two squads, each squad assigned a different value



Imitator group: a group whose value equals the mean of the perturbation group, while the collector does not estimate its mean or frequency.

Experiments

- **Audited LDP protocols**

  Non-interactive protocols: PCKV-UE, PCKV-GRR
  Interactive protocols (PrivKVM / PrivKVM*): CPP-UE, CPP-GRR; CPP-UE*, CPP-GRR*

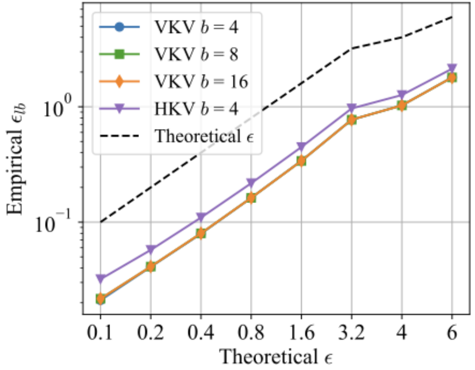
- **Input Construction**

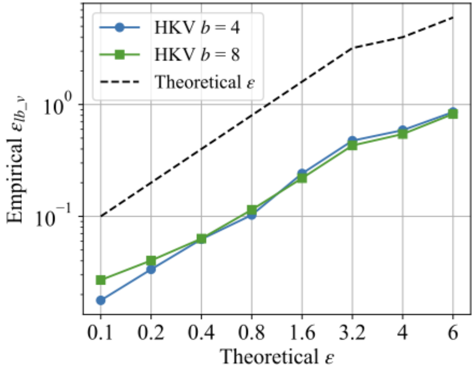
  PCKV-UE, PCKV-GRR: kv_1 = <k=k_1, $v = 1$>, kv_2 = <k=k_2, $v = -1$> $k_1 \neq k_2$
  CPP-UE and CPP-GRR: kv_1 = <k=k, $v = 1$>, kv_2 = <k=k, $v = -1$>,

- **Observed Reports by Analyzer(after perturbation):**

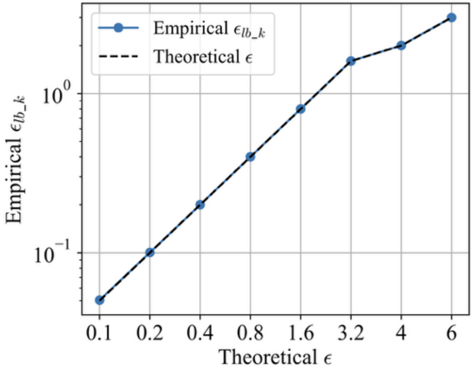
  UE → binary vector (not one-hot)
  GRR → randomized key + randomized value

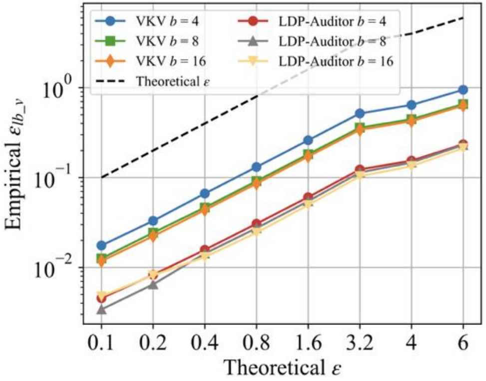
Experiments





- For PCKV-GRR, large N_key causes more privacy leakage.
- HKV-Auditor is inaccurate for UE with a large bit length b, while VKV-Auditor is stable.





- Our KV-Auditor is tighter than the LDP-Auditor.
- The theoretical of keys in CPP is tight.

[1] Arcolezi, Héber Hwang, and Sébastien Gambs. "Revealing the True Cost of Local Privacy: An Auditing Perspective." CoRR (2023).

Experiments

Theoretical	Empirical ϵ_{lb}				
ϵ	$c = 1$	$c = 2$	$c = 3$	$c = 4$	$c = 5$
0.1	0.0068	0.0092	0.0134	0.0140	0.0139
0.2	0.0076	0.0152	0.0214	0.0234	0.0252
0.4	0.0080	0.0298	0.0366	0.0410	0.0406
0.8	0.0148	0.0460	0.0646	0.0710	0.0752
1.6	0.0538	0.1224	0.1237	0.1257	0.1261
3.2	0.3064	0.4241	0.4248	0.4250	0.4265
4	0.5020	0.5580	0.5569	0.5568	0.5553
6	1.0392	0.6218	0.6343	0.6390	0.6475

In CPP-UE, privacy leakage decreases with iterations due to mean convergence.

Theoretical	Empirical ϵ_{lb}				
ϵ	$c = 1$	$c = 2$	$c = 3$	$c = 4$	$c = 5$
0.1	0.0096	0.0078	0.0082	0.0070	0.0071
0.2	0.0165	0.0112	0.0098	0.0092	0.0085
0.4	0.0270	0.0161	0.0164	0.0153	0.0143
0.8	0.0537	0.0299	0.0275	0.0265	0.0237
1.6	0.1240	0.0558	0.0528	0.0481	0.0495
3.2	0.3090	0.1103	0.1069	0.1078	0.1051
4	0.4219	0.1431	0.1408	0.1364	0.1362
6	0.7327	0.2352	0.2292	0.2296	0.2281

In SHKV-Auditor, empirical ϵ_{lb} decreases with iterations as the mean converges, with the first iteration showing the highest leakage.

Summary

- We introduce a KV-Auditor framework to estimate the ϵ_{lb} of LDP protocols for key-value data.
- Based on this framework, we propose HKV-Auditor and VKV-Auditor for non-interactive protocols, SKV-Auditor for interactive protocols.
- The upper bound for GRR is tighter than that for UE, indicating greater room for improvement in UE.

Thank you!

KV-Auditor | CIKM2025

arxiv.org/abs/2508.11495
github.com/JingnanXu97/KV-Auditor

jnxu@ruc.edu.cn