Scaling Cryptographic Techniques by Exploiting Data Sensitivity at a Public Cloud

Sharad Mehrotra[1], Shantanu Sharma[1], and Jeffrey D. Ullman[2]
[1]University of California, Irvine. [2]Stanford University.

Goal: Increase efficiency of cryptographic techniques

1 Existing Problem

Cryptographic techniques are:

i. Not efficient

ii. Prone to various attacks

Technique	Time	Resilient to attacks		
		Size	Workload-skew	Access-pattern
DET Enc.	1.43x			
Non-DET Enc.	2.1x			
Distributed Searchable Enc.	3281x			✓
SGX	6724x			
Full-Retrieval	11235x	✓	✓	✓
Homomorphic + ORAM	>11235x			✓

x: The time to search a predicate in cleartext.
✓: A technique is resilient to a given attack.

2 Partition Computation

- Partition the data into sensitive and non-sensitive
- Sensitive data is cryptographically secure
- Non-sensitive data is in cleartext

Secure Sensitive data (at the public cloud)

	Name	Department
t_1	E(Adam)	E(Defense)
t_2	E(John)	E(Security)
t_3	E(Clark)	E(Crypto)
t_4	E(Lisa)	E(Defense)

Insecure non-sensitive data (at the public cloud)

	Name	Department
t_5	John	Testing
t_6	Eve	Testing
t_7	David	Design
t_8	Clark	Design

Inference Attacks due to Data Partitioning

Adversarial view
what the adversary observes

Query value	Retuned tuples	
	From sensitive data	From non-sensitive data
John	t_2	t_5
Adam	t_1	Null

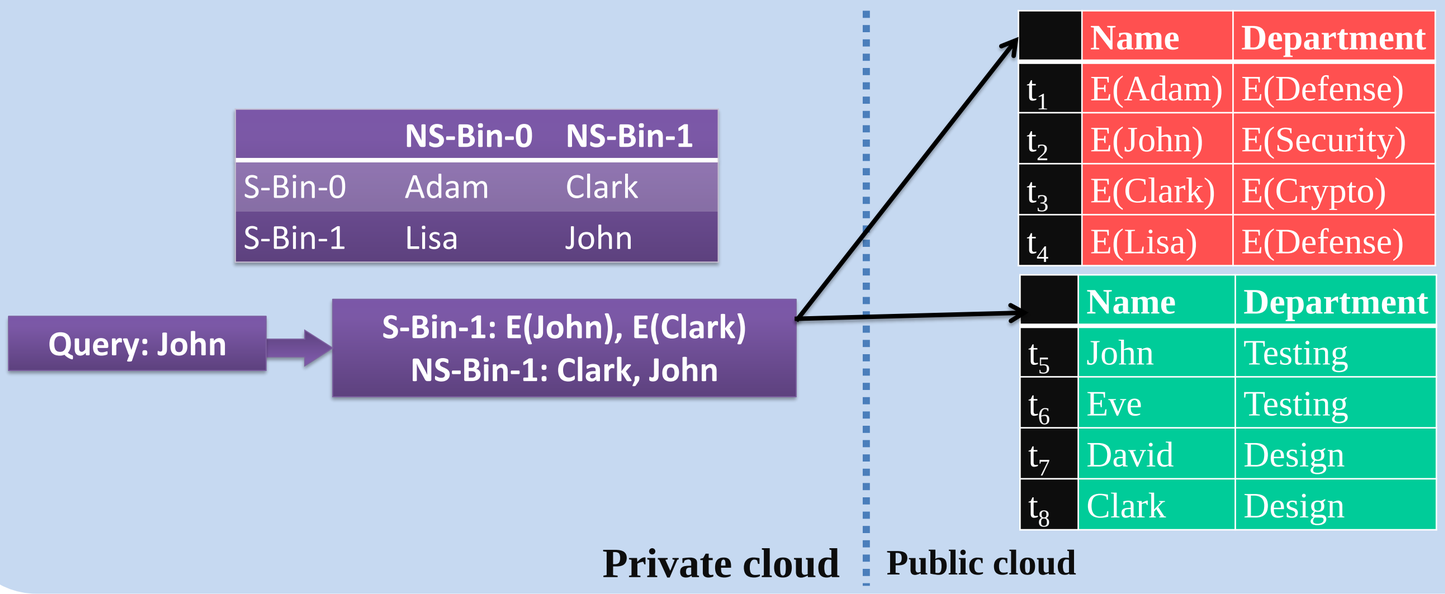
3 Query Binning

Partition Data Security

- No linking of sensitive and non-sensitive values
- Not revealing #tuples with each sensitive value

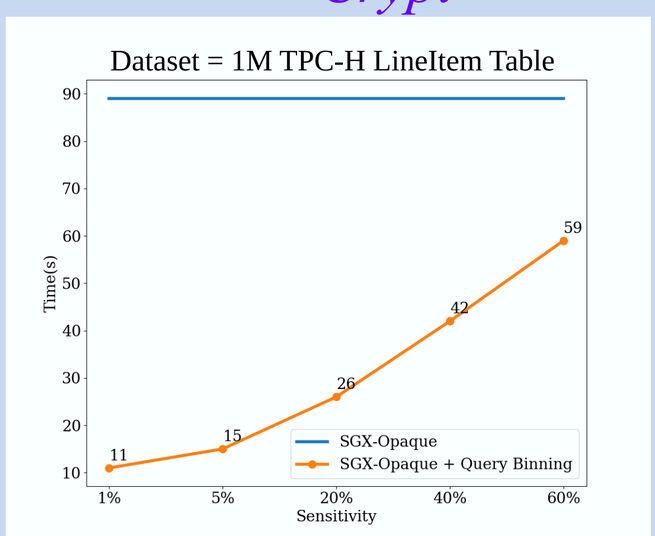
Idea of Query Binning

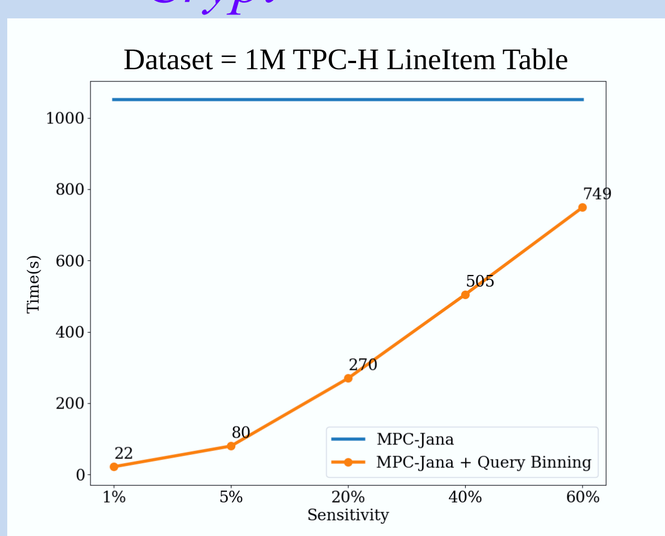
- Distribute "values" into a matrix
- Rows become sensitive bins
- Columns become non-sensitive bins



4 Performance

$$\eta = \frac{Cost_{crypt}(|SB|,S)}{Cost_{Crypt}(1,D)} + \frac{Cost_{plain}(|NSB|,NS)}{Cost_{Crypt}(1,D)}$$





5 Interesting Facts

- Works for any number of sensitive and nonsensitive values
- Improves an underlying cryptographic technique by preventing output-size and frequency-count attacks
- Supports conjunctive selection, join, and range queries

6 Reference

- S. Mehrotra et al. Partitioned Data Security on Outsourced Sensitive and Non-sensitive Data. ICDE, 2019.