Fine-grained Sharing of Encrypted Sensor Data on the Cloud

SeSaMe

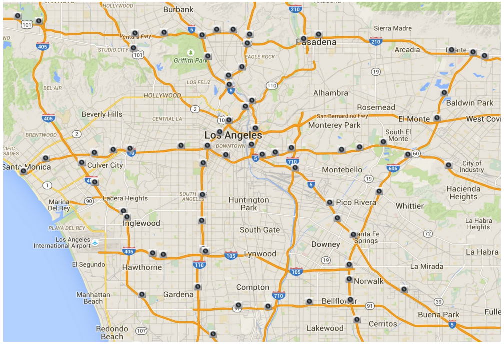
Motivation

Data thef and privacy concerns require sensitive data to be kept encrypted. However, this brings forth technical challenges on fine-grained sharing.

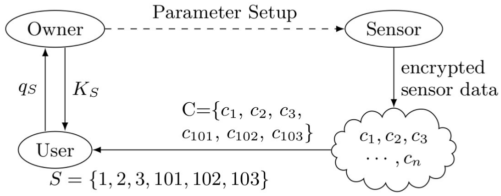
Existing cryptographic schemes stop short on addressing these challenges.

Our work proposes an optimal and scalable solution for the problem at hand.

An Example



System Model



Parameter Setup

Owner

Sensor

encrypted sensor data

q_S

K_S

C={c_1, c_2, c_3, c_{101}, c_{102}, c_{103}}

c_1, c_2, c_3 $\cdots, c_n$

User

$S = \{1, 2, 3, 101, 102, 103\}$

Our Solution

1. Built on top of Key-Aggregation Cryptosystem and improves its performance by orders of magnitude.
2. Presents linear time reconstruction algorithm for range and sub-sampling queries.
3. Evaluates optimal computational plan for reconstructing general queries.
4. Enables trade-off between number of aggregated keys and reconstruction time.

Performance Analysis

		ABE	KAC	Ours
Encrypt	Mult.	$n(4d+2)$	$2n$	$2n$
	Exp.	$n(4d+2)$	$3n$	$3n$
	Pairing	n	n	n
QueryResponse	Mult.	d	n	n
	Exp.	$3d$	1	k
	Pairing	0	0	0
Reconstruct	Mult.	nd	$O(n^2)$	$O(n)$
	Exp.	nd	0	0
	Pairing	$2nd$	$n+1$	$n+k$

Table 1: Performance Analysis of different approaches.

Experimental Study

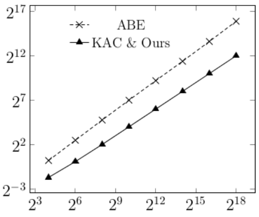


Figure 1: Encryption time

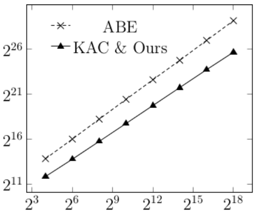


Figure 2: Storage Space

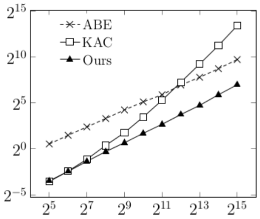
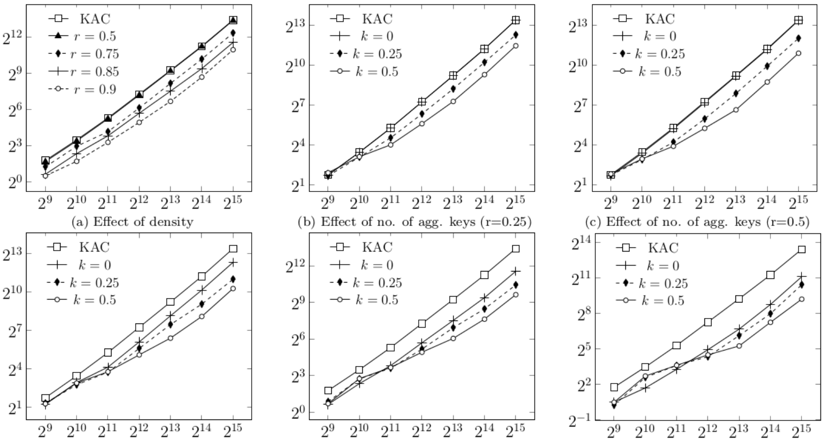


Figure 3: Q1 & Q2 reconstruction time



(a) Effect of density

(b) Effect of no. of agg. keys (r=0.25)

(c) Effect of no. of agg. keys (r=0.5)

(d) Effect of no. of agg. keys. (r=0.75)

(e) Effect of no. of agg. keys. (r=0.85)

(f) Effect of no. of agg. keys. (r=0.9)

Figure 4: Q3 reconstruction time

Principle investigators: Prof. Ee-Chien Chang

NUS National University of Singapore

CONTACT PERSON: Dr Lekha Chaisorn (Deputy Executive Director)
TEL.: (65) 6516 3916 FAX: (65) 6773 5018 EMAIL: idmlekh@nus.edu.sg
ADDRESS: SeSaMe Centre, I³ Building, #02-02,
Interactive Digital Media Institute,
National University of Singapore,
21 Heng Mui Keng Terrace, Singapore 119613
WEBSITE: http://sesame.comp.nus.edu.sg