An analytical study for sensor service providers to keep their user's security

Oct. 2012

T a k a m i c h i A s o u

I n s t i t u t e o f I n f o r m a t i o n S e c u r i t y

Contents

1. Intro
2. Sensor Service
3. My motivation of research
4. I am worried about privacy violation
5. What is sensor data?
6. Protect privacy
7. Scenarios to use cloud effectively
8. Scenarios and Security requirements
9. Methods x Scenarios
10. Outro

2. Sensor services

	Purpose of the set	Kind of sensor
Traffic, Vehicle	•Control of vehicle •Maintain vehicle •Navigation system •JAM prediction •Avoid car accident	【power train control】 Throttle position, Accelerator , Intake pressure, Fuel pressure, … 【Vehicle Control】 laser radar, Steering, Throttle, Acceleration, … 【Body control】 Back sonar, Corner sonar, … 【Communication】 laser radar, GPS, VICS, Gyro, …
Mobile	•Performance improvement •Utility value improvement	GPS, Gyro, Thermometer, Acceleration, Barometer, Illuminometer. …
Smart House	•HEMS •Appliances control	Smart meter Gus, water, Motion, Door, Camera …

http://e-public.nttdata.co.jp/topics_detail2/id=659
http://www.denso.co.jp/ja/aboutdenso/technology/dtr/v11_1/files/disseration14itp6.pdf
http://www.sei.co.jp/products/info/its_jp.pdf
http://easy.mri.co.jp/20120228.html
http://www.jipdec.or.jp/dupc/forum/eships/results/doc/h21project_report1-1.pdf

2. Sensor services

	Sensor Owner	Who set the sensor？	Who collect the data? (Sensor service provider)	Who want to use the data? (Other Service Provider)	Who is the target to sense?
Traffic, Vehicle	Vehicle Owner	Auto Manufacturer	Auto Manufacturer （government）	Government	Vehicle User (family, friends..)
			Auto Manufacturer	Insurance	
			Auto Manufacturer	Auto Manufacturer	
			Auto Manufacturer	Owner, owner's Family	
Mobile	Mobile Owner	Mobile Maker Career	Application Provider	End User	Mobile User
			Career	Career	
			Career	Government	
Smart House	Power Company or Sensor Owner	Power Company or Sensor Owner	Power Company	Power Company	Family (not individual)
			Government	Government	
			Career	Sensor Owner	

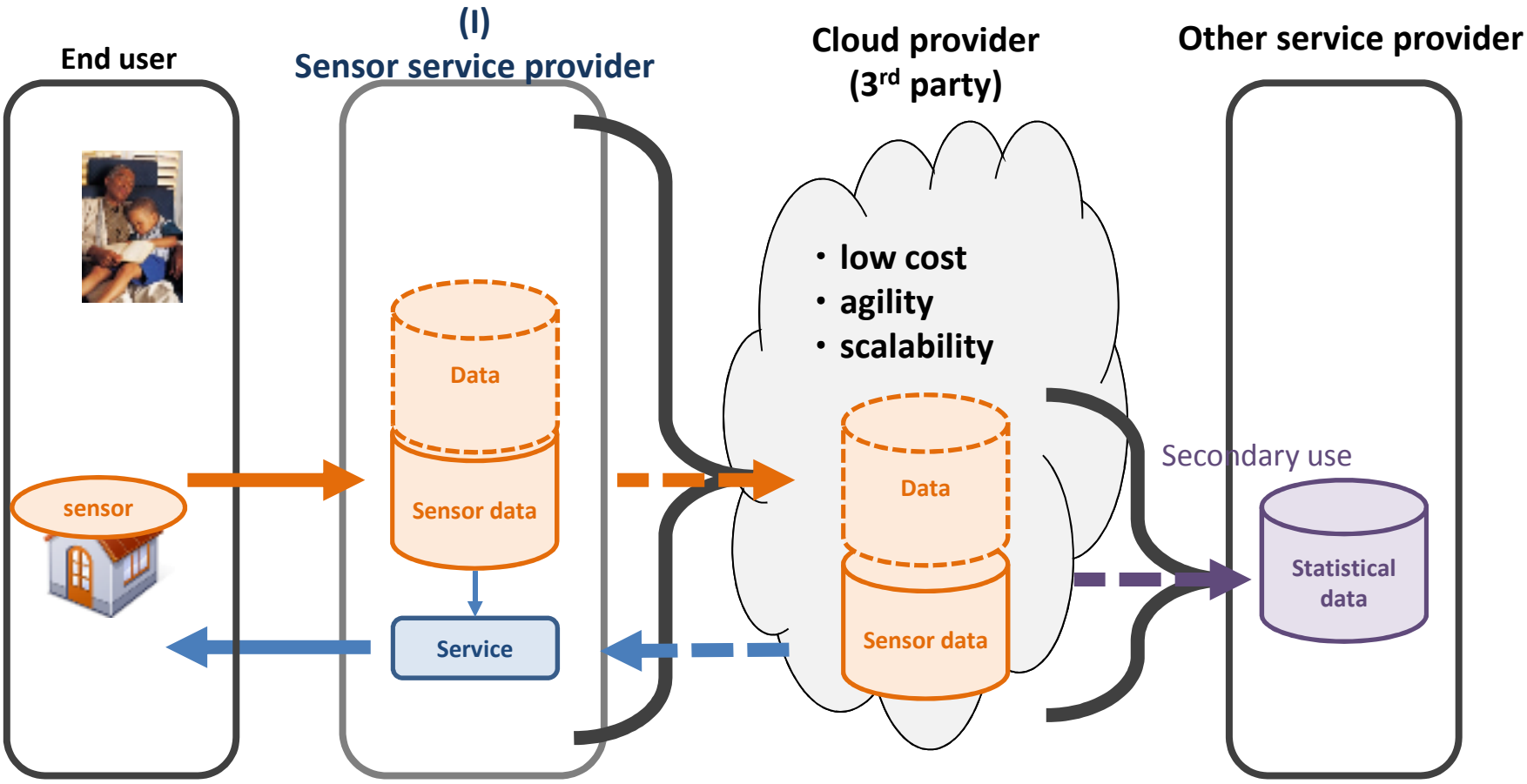
- The target is not only the owner
- Someone who utilize sensor data is not only the owner of sensor, target Sensor service provider recognize this complicated situation.

3. My motivation of research

3. My motivation of research

As a sensor service provider

Because data volume is increasing, I want to use cloud securely at low cost, and I want the data to be used for secondary use for next business.



There might be some concerns to use cloud…

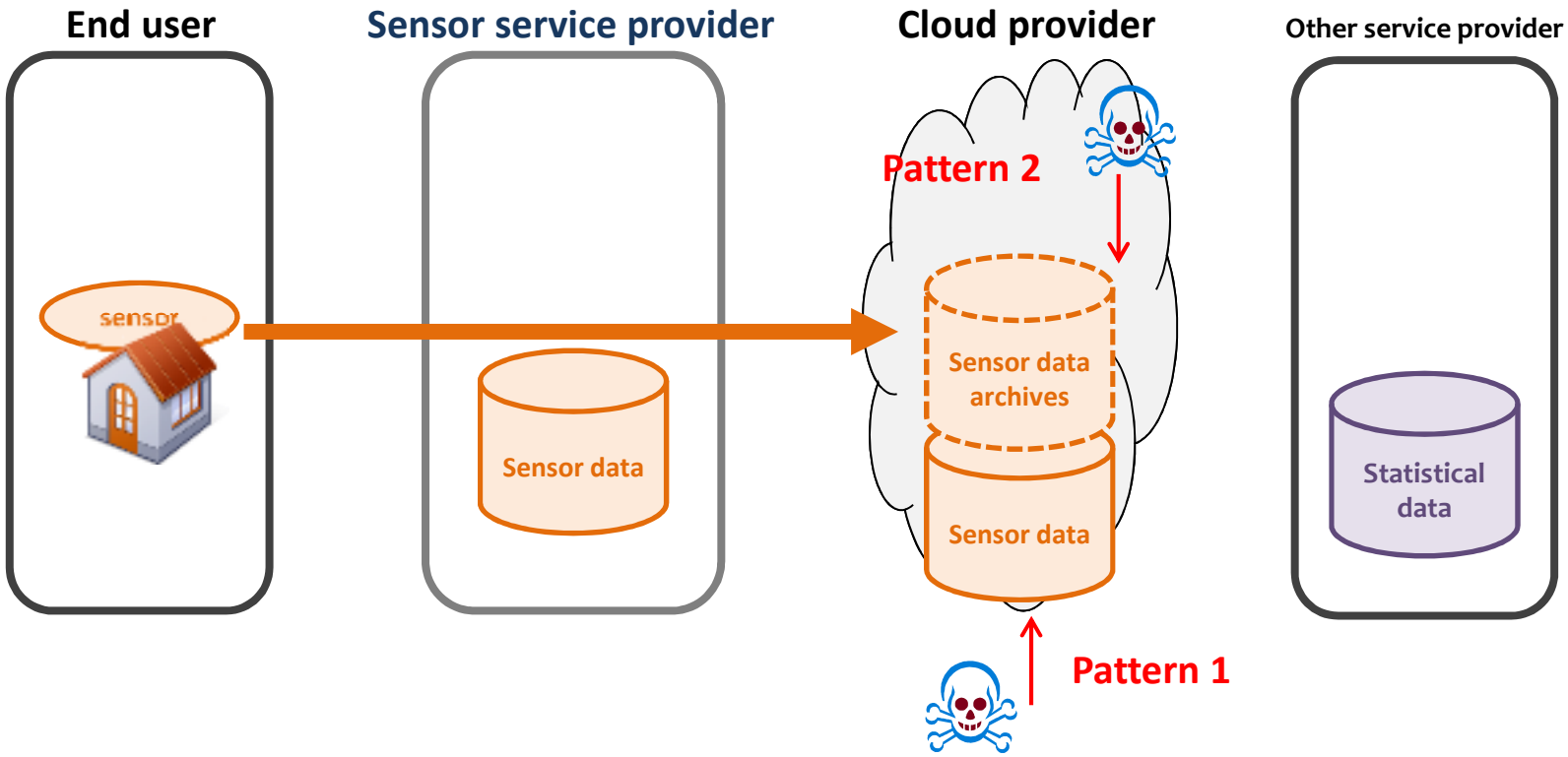
4. I am worried about privacy violation

■Most important concern is data leakage when I use cloud

I am worried about two types of patterns.

Pattern 1 : External attacker attacks cloud
Pattern 2 : Internal attacker attacks cloud

Assume that this would absolutely happen.
I want my customer not to be violated their privacy.



5. What is sensor data?

■Sensor data is divided into two kinds.

1. Personal information
2. Sensitive data (information)

1. Personal Information

- Customer Information

We have to protect this kind of information and follow the Japanese law named
"Act concerning protection of Personal Information"

Especially, article 19 ~ 23

http://www.japaneselawtranslation.go.jp/law/detail_main?id=130&vm=4&re=

This law and my assumption,
I have to decide very carefully whether I use cloud for it or not.

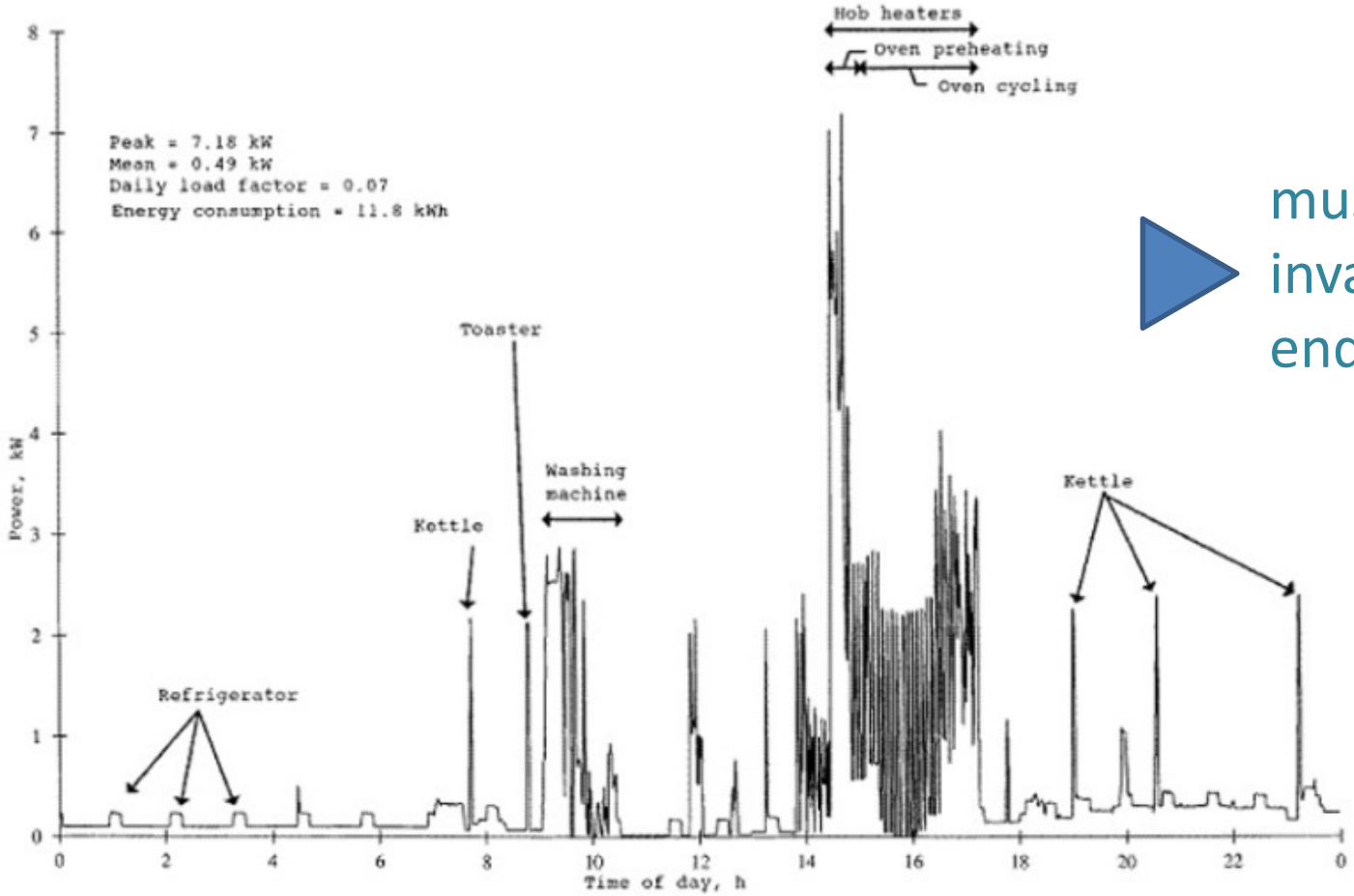
5. What is sensor data?

2. Sensitive data

http://articles.chicagotribune.com/2012-09-27/news/ct-tl-naperville-smart-meter-arguments-20120927_1_naperville-smart-meter-awareness-analog-meters-security-and-privacy-concerns

- physical data, religion, race, medical record, …
- Sensor data (electric, gas, water) This kind of data could show privacy

But this data needs a fixed term. Not just one, single data



must prevent invasion of end users privacy

http://spectrum.ieee.org/energy/the-smarter-grid/privacy-on-the-smart-grid

6. Protect privacy

What is the meaning to protect end user's privacy from leaking of their sensitive data?

- prevention the identifying individual
- prevention the invasion of privacy

How can I ?

CustomerID	ProductID	Time to send	Time to be measured	Volume (mA)
ABCD1234	ID00001	2012/7/1 10:10:01:21	2012/7/1 10:00:00	3
ABCD9876	ID00002	2012/7/1 10:10:03:08	2012/7/1 9:58:57	7

● Anonymity
k-anonymity
l-diversity

● Reconstruction (perturbation)
Randomization
Swapping

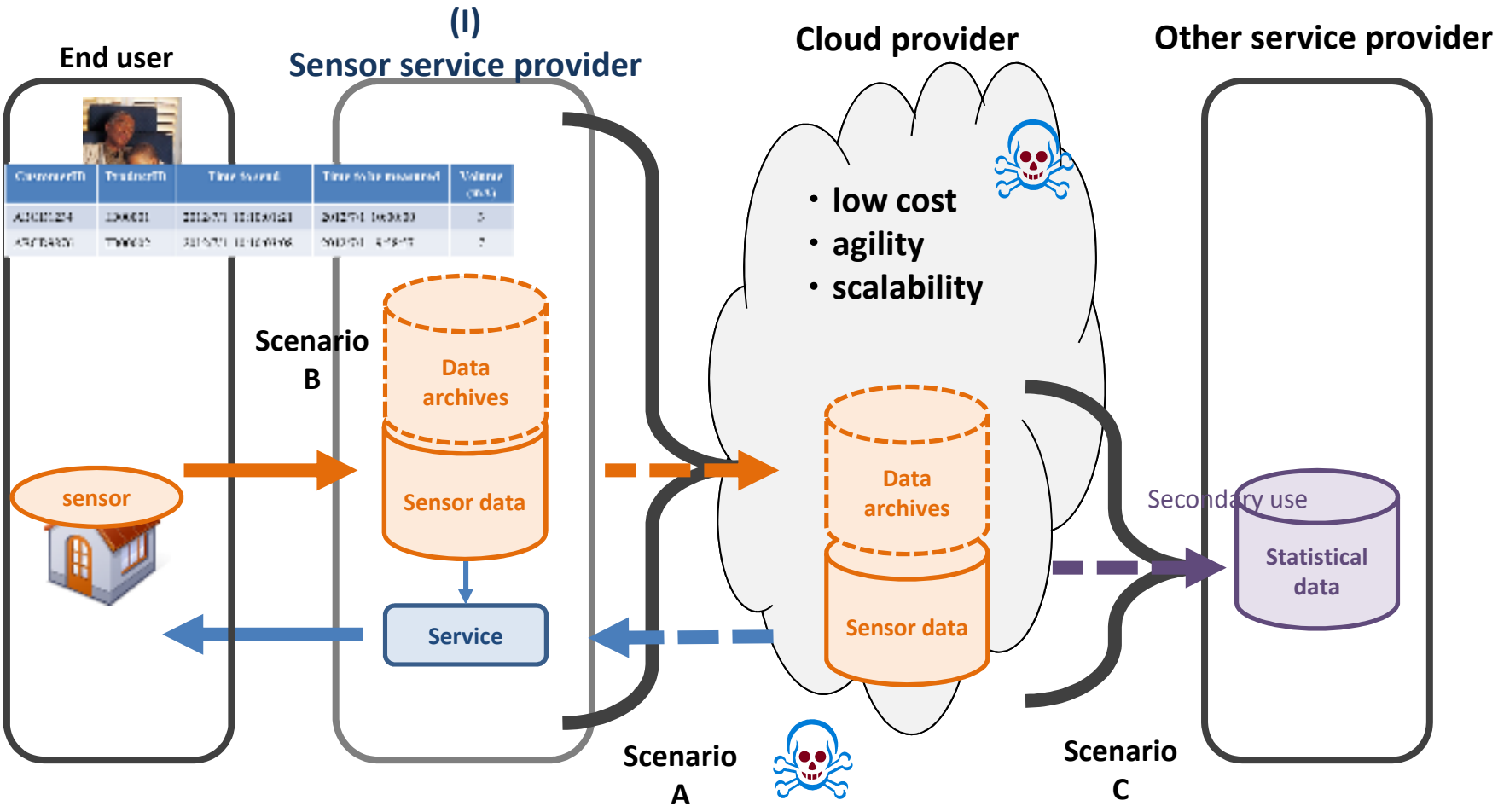
perturbation that converts attributes *probabilistically*
reconstruction that derives a statistic from a perturbed data

Depend on how to use Cloud & use for what

Secure multiparty computation
Functional Encryption

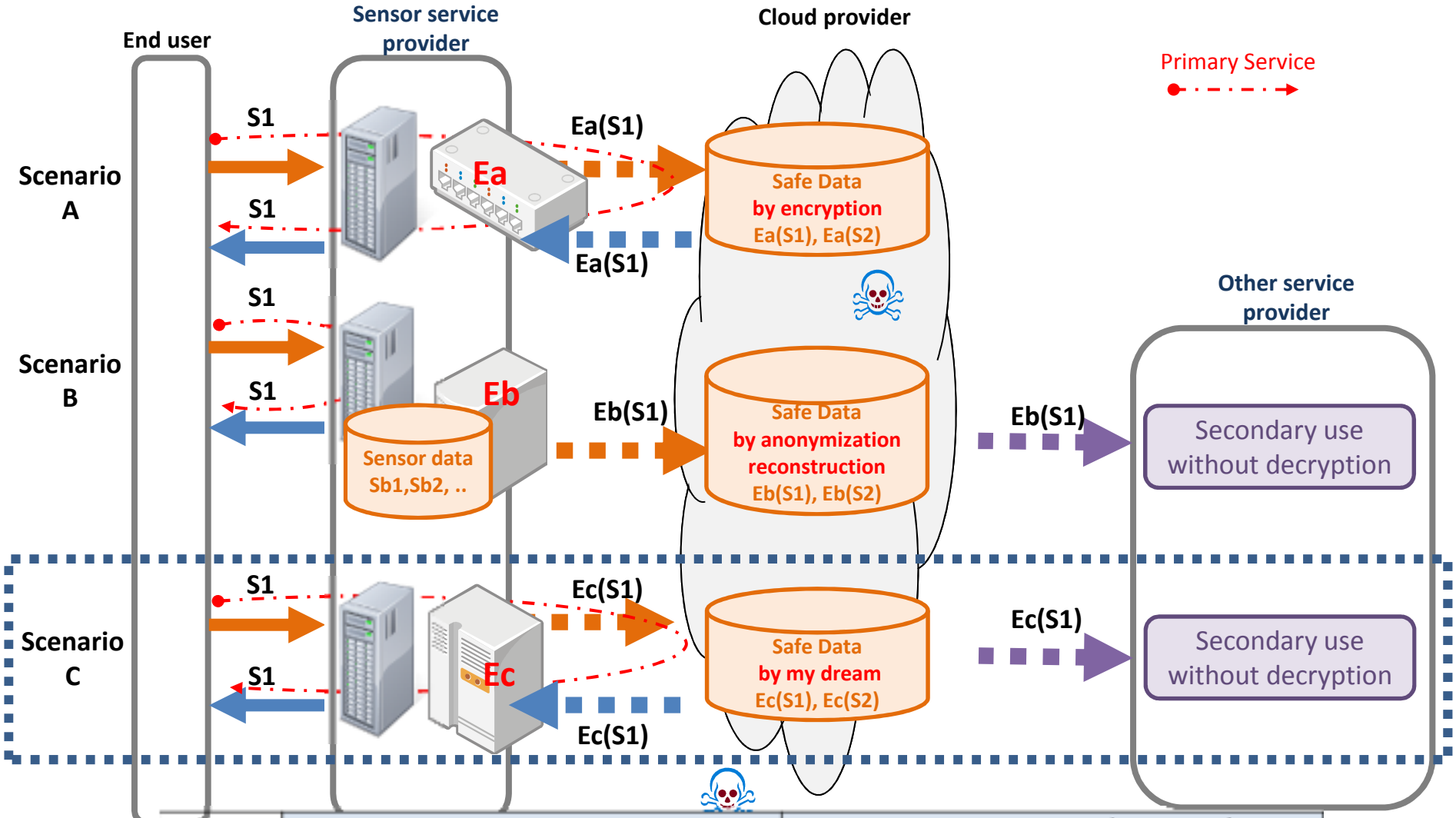
homomorphic encryption
Shamir's Secret Sharing

7. Scenarios to use cloud effectively



In the case,
Sensor service provider has notified the end users that
modified sensor data, which is of course eliminated identifying individual and sensitive factors, such as statistical data, would be used for secondary use with specific other service providers.

8. Scenarios and Security requirements



	Content	Security requirements (secure + ...)
Scenario A	Primary data storage	Getting row data back.
Scenario B	Secondary usage Infra	Statistical data for secondary use
Scenario C	Primary data storage and secondary usage Infra	Getting row data back Statistical data for secondary use

9. Methods x Scenarios

■Table: Method x Scenarios

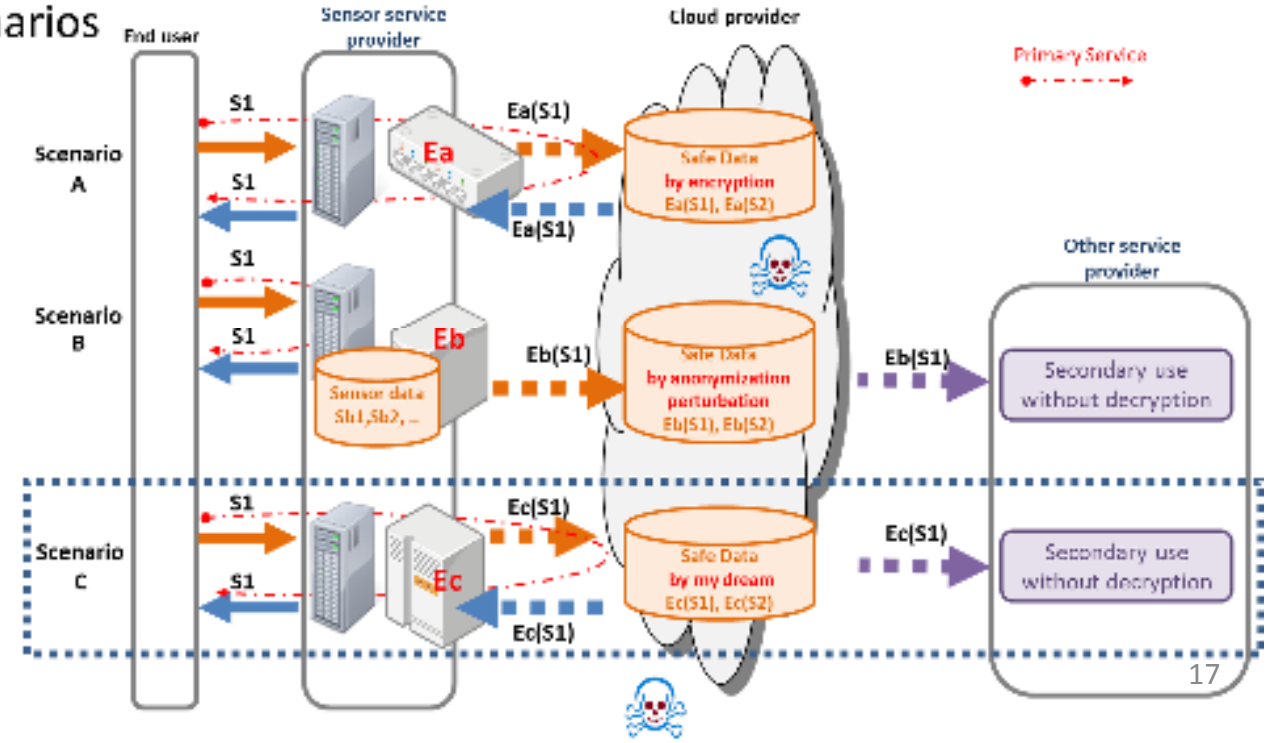
	Anonymization	Reconstruction	Encryption
Scenario A	-	-	○
Scenario B	○	○	-
Scenario C	-	-	-

○ satisfy my security requirements
- hardly satisfy my security requirements

●On Scenario C,
you are hardly able to use anonymization, Reconstruction.
because both wouldn't end up with getting out row data of.

10. outro

1. Intro
2. Sensor Service
3. My motivation of research
4. I am worried about privacy violation
5. What is sensor data?
6. Protect privacy
7. Scenarios to use cloud effectively
8. Scenarios and Security requirements
9. Methods x Scenarios
10. Outro



Fin.

k-anonymity

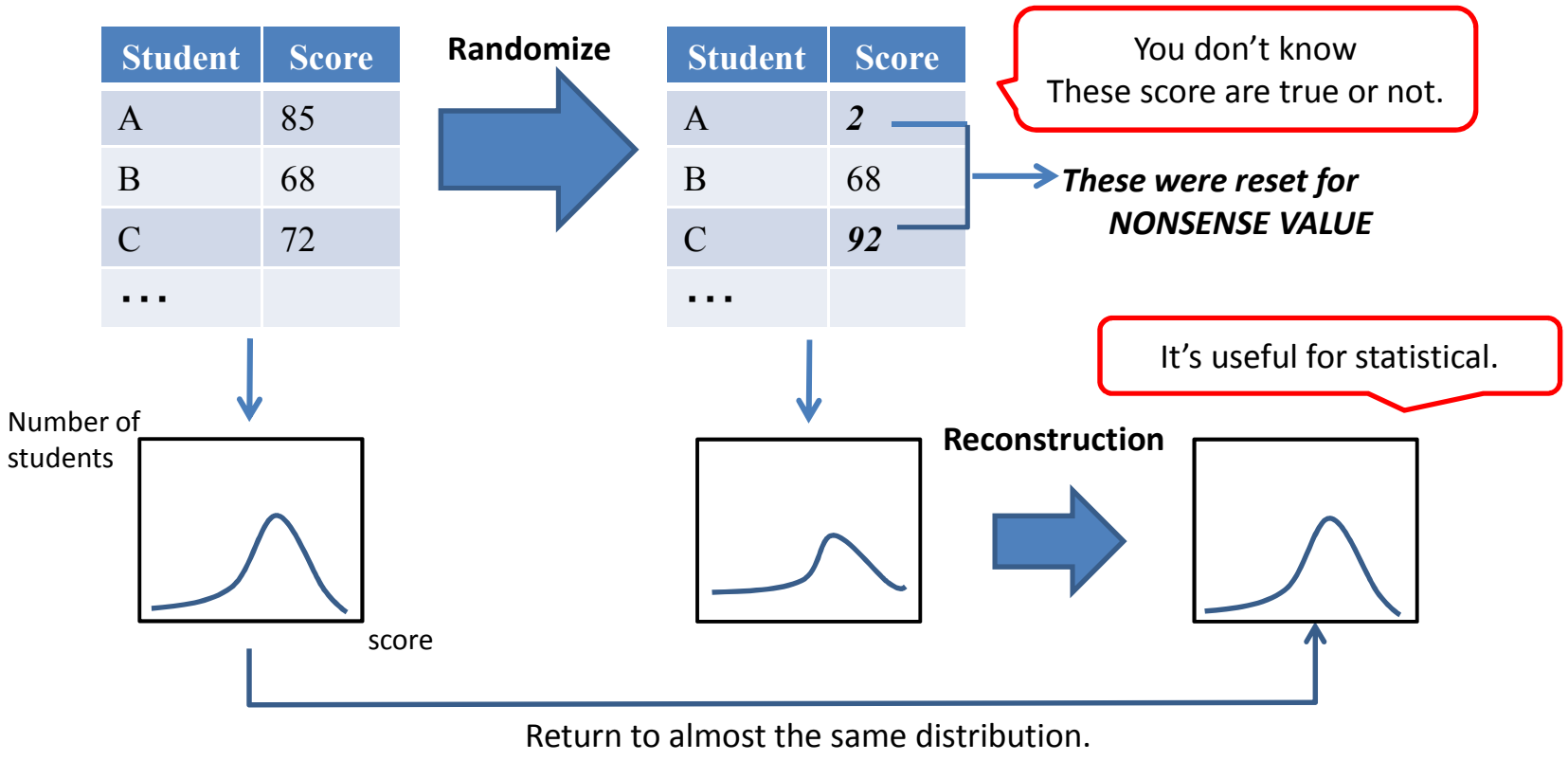
Definition 3. *k*-anonymity
Let RT(*A1*,...,*An*) be a table and QI_{RT} be the quasi-identifier associated with it. RT is said to satisfy *k*-anonymity if and only if each sequence of values in RT[QI_{RT}] appears with at least *k* occurrences in RT[QI_{RT}].

	Race	Birth	Gender	ZIP	Problem
t1	Black	1965	m	0214*	short breath
t2	Black	1965	m	0214*	chest pain
t3	Black	1965	f	0213*	hypertension
t4	Black	1965	f	0213*	hypertension
t5	Black	1964	f	0213*	obesity
t6	Black	1964	f	0213*	chest pain
t7	White	1964	m	0213*	chest pain
t8	White	1964	m	0213*	obesity
t9	White	1964	m	0213*	short breath
t10	White	1967	m	0213*	chest pain
t11	White	1967	m	0213*	chest pain

Figure 2 Example of *k*-anonymity, where *k*=2 and QI={*Race*, *Birth*, *Gender*, *ZIP*}

L. Sweeney. *k*-anonymity: a model for protecting privacy. *International Journal on Uncertainty, Fuzziness and Knowledge-based Systems,* 10 (5), 2002; 557-570.

Reconstruction method



- 中道　理，河合　基伸，“特集　センサ・データを解放せよ　ユーザを”不幸“にしないための処方箋，”日経エレクトロニクス，no.1083，5-28，pp.25-50，May.2012　をベースに作成