قطب علمی رمز

انجمن رمز ایران

برون‌سپاری امن پایگاه‌داده و رویکردهای تامین محرمانگی

رامین بهلولی

دانشکده مهندسی کامپیوتر– دانشگاه صنعتی شریف

rbohlooli@ce.sharif.edu

پژوهشکده امنیت رایاسامانه های شریف (پارسا شریف)

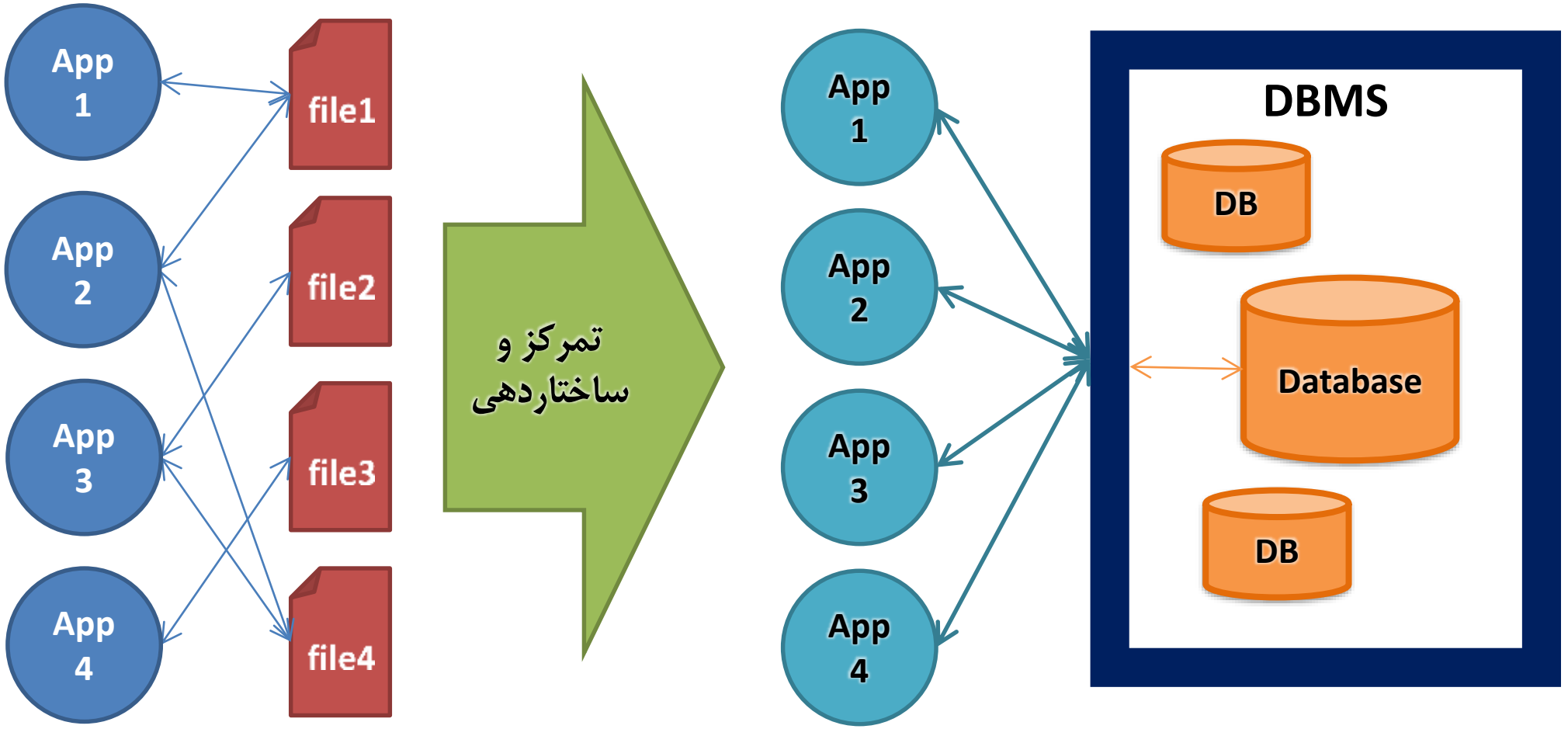
چشم‌انداز

- مقدمه
  - مروری بر مفاهیم اوّلیه پایگاه‌داده
  - پایگاه‌داده به عنوان سرویس
  - چالش‌های امنیتی
- رویکردهای تأمین محرمانگی
  - روش‌های مبتنی بر رمزگذاری
  - روش‌های مبتنی بر چندپارگی
- جمع‌بندی

مقدمه

مروری بر مفاهیم پایگاه‌داده

مروری بر مفاهیم پایگاه‌داده



مروری بر مفاهیم پایگاه‌داده (ادامه)

id	name	city	date
5	Ali	Tehran	1/1/14
6	Naser	Shiraz	2/2/13
10	Ramin	Tabriz	3/8/16
1	Javad	Rasht	3/2/15
2	Ahmad	Zabol	1/4/12
0	Reza	Ahvaz	2/5/16

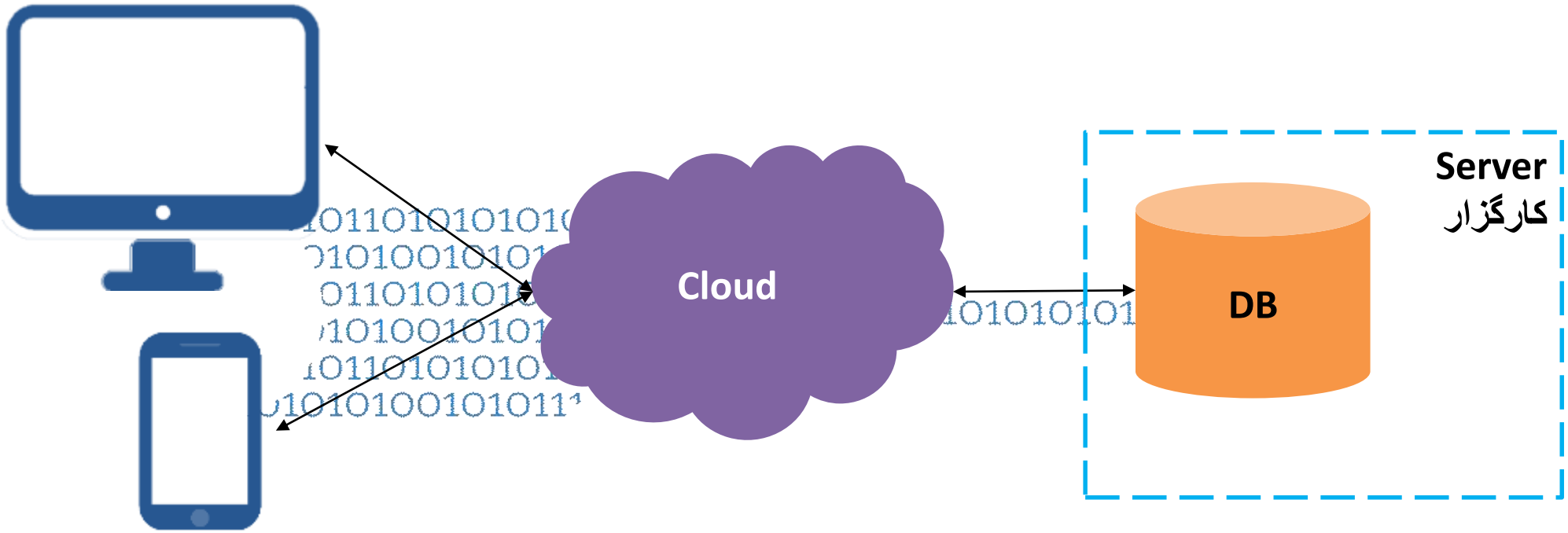
پایگاه‌داده رابطه‌ای

- سازمان‌دهی داده‌ها در قالب تعدادی جدول
  - موجودیت‌های ساخت‌یافته در قالب مجموعه‌ای از صفات
  - هر صفت دارای نوع (عدد، رشته، تاریخ و...)
- کار با داده در قالب پرسمان (Query)
  - زبان SQL

```
SELECT * FROM table1 WHERE date BETWEEN 1/1/13 AND 2/2/14
SELECT city FROM table1 WHERE city LIKE %r_%
INSERT INTO table1 VALUES (0, 'Reza', 'Ahvaz',2/5/16)
UPDATE table1 SET id = 10 WHERE name = 'Ramin'
DELETE FROM table1 WHERE id > 3
```

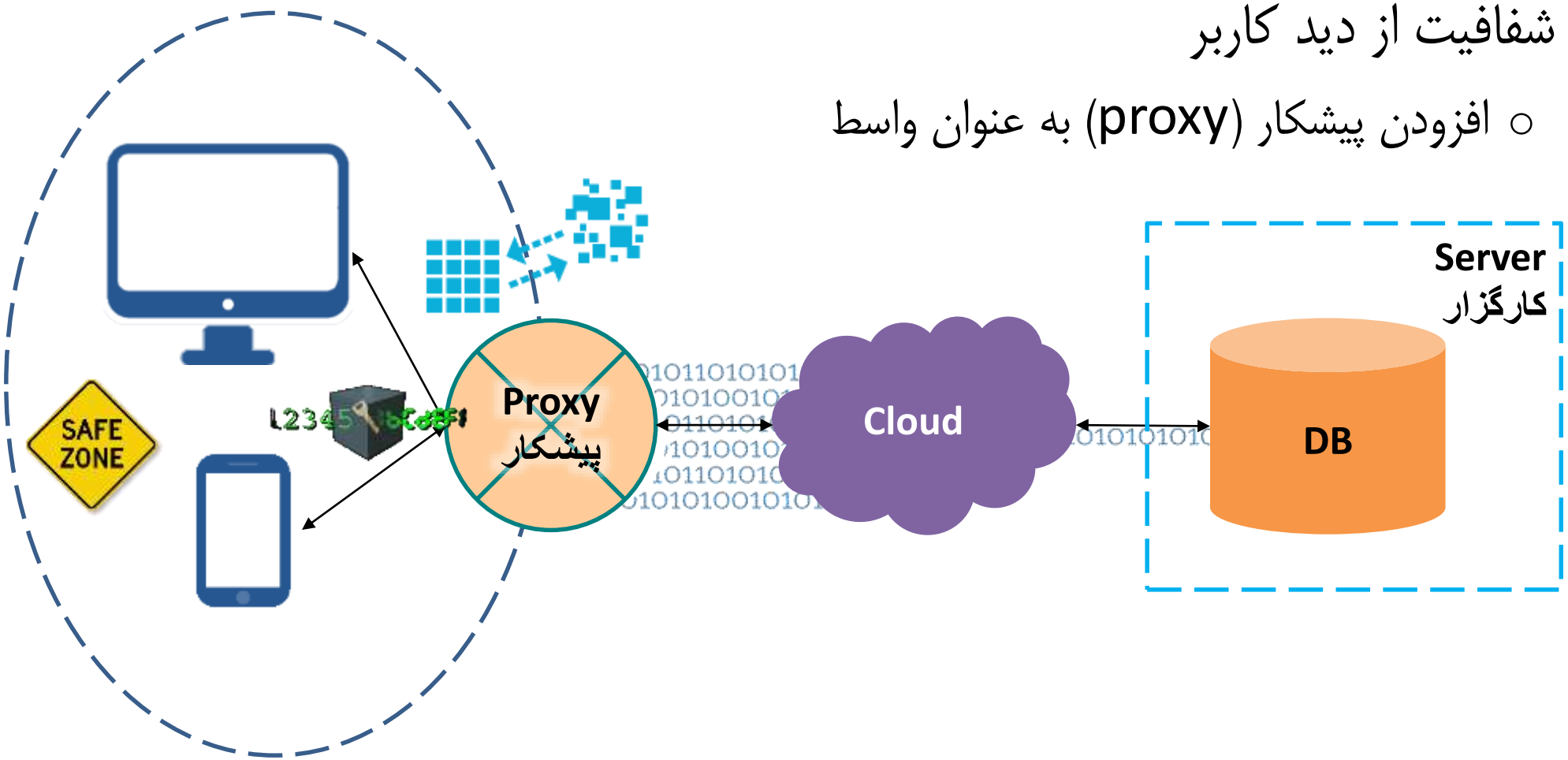
پایگاه داده به عنوان سرویس

- کاهش هزینه‌ها
- دسترس‌پذیری



برون‌سپاری امن پایگاه داده

- افزودن ملاحظات امنیتی
- شفافیت از دید کاربر
  - افزودن پیشکار (proxy) به عنوان واسط



چالش‌ها

- محرمانگی (confidentiality)
- جامعیت داده (data integrity)
- کنترل دسترسی (access control)
- ...
  - واگذاری به کارگزار
    - اعمال در سمت پیشکار
    - ترکیب با روال رمزگذاری
      - رمزگذاری ویژگی‌بنیاد
      - مدیریت کلید

انواع مدل‌های کارگزار

- معتمد اما کنجکاو
  - وفاداری به روال کار و پروتکل تعیین شده
  - فقط نیاز به محرمانگی
- نا معتمد
  - امکان تخطی از پروتکل
    - حذف بخشی از جواب
    - اعلام عدم وجود داده
    - ...
  - نیاز به محرمانگی و جامعیت(+ کنترل دسترسی و...)

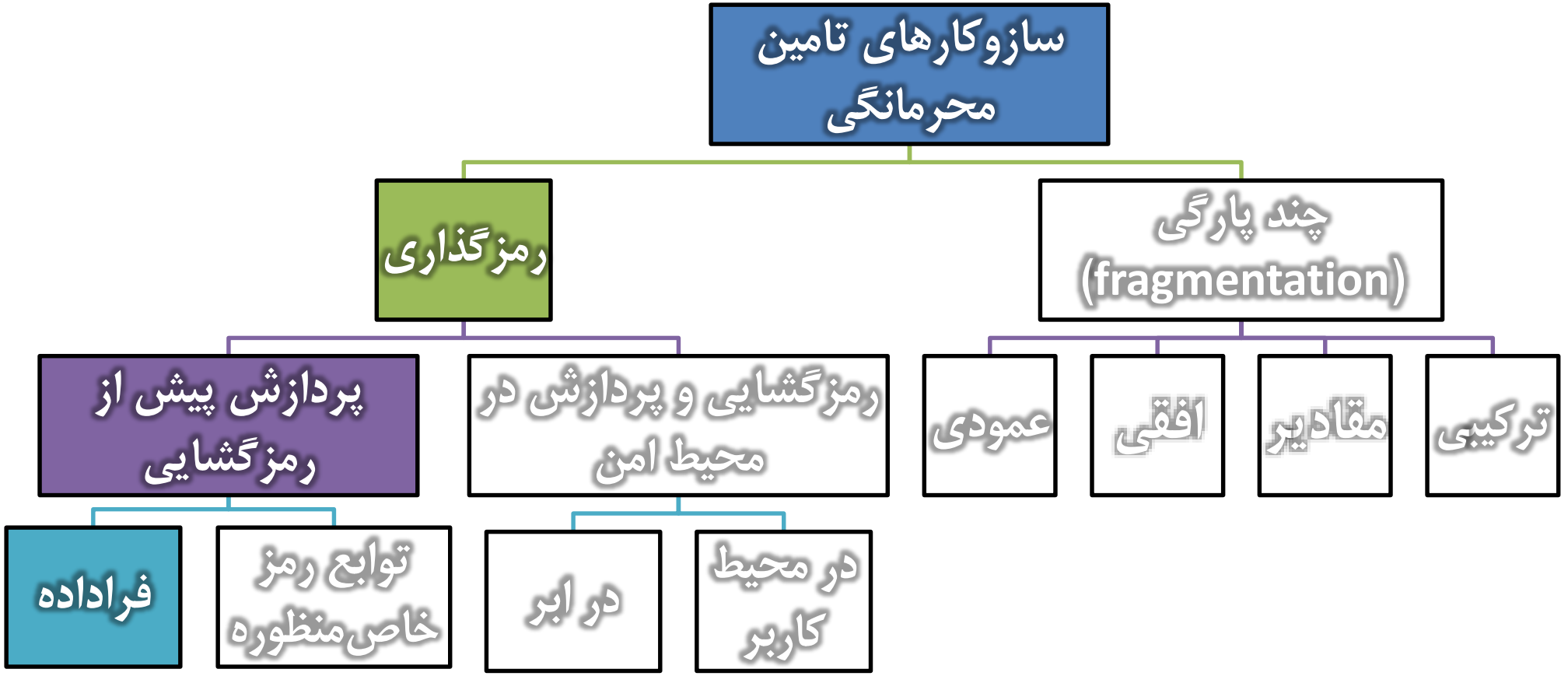
رویکردهای تأمین محرمانگی

دسته‌بندی کلی

دسته‌بندی کلی

سازوکارهای تامین محرمانگی

رویکردهای تأمین محرمانگی



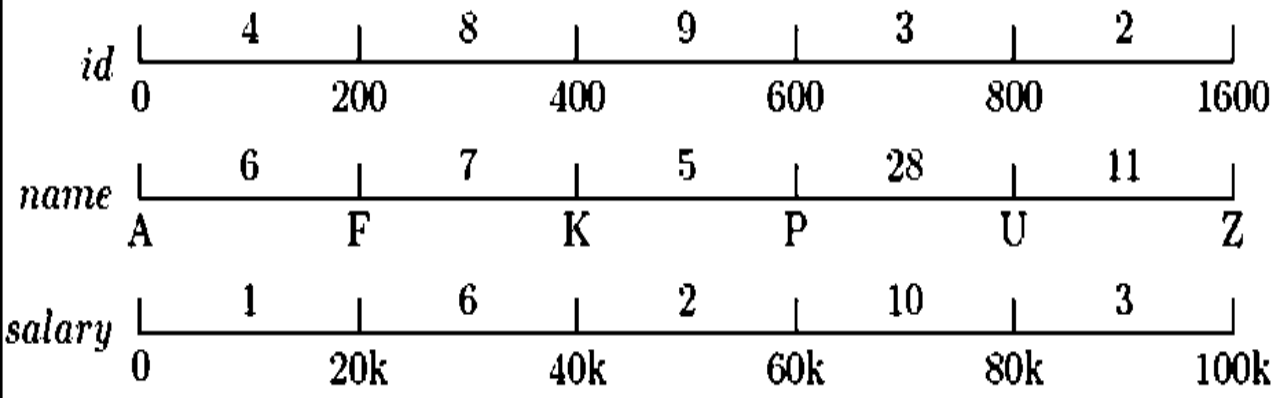
فراداده

- تعریف: داده‌ای برای توصیف ویژگی(های) داده(های) دیگر
- شاخص (index): نوع خاصی فراداده
  - افزایش سرعت بازیابی (عدم نیاز به جستجوی پویشی)
  - افزایش هزینه درج و حذف
- مراحل
  ۱. ساخت شاخص (index) از روی داده آشکار
  ۲. رمزگذاری داده‌های واقعی و قرار دادن در کارگزار
  ۳. قرار دادن شاخص در کنار داده رمزشده در کارگزار

فرادداده

- انواع
  - مبتنی بر بازه‌گذاری (bucket-based)
  - مبتنی بر چکیده‌سازی (hash-based)
  - مبتنی بر درخت B^+
  - ...

Id	Name	Salary
23	Tom	70000
860	Mary	60000
320	Tony	50000
875	Jerry	5600



Enc-tuple	Id^S	$Name^S$	$Salary^S$
010011...	4	28	10
110010...	2	5	10
001110...	8	28	2
100011...	2	7	1

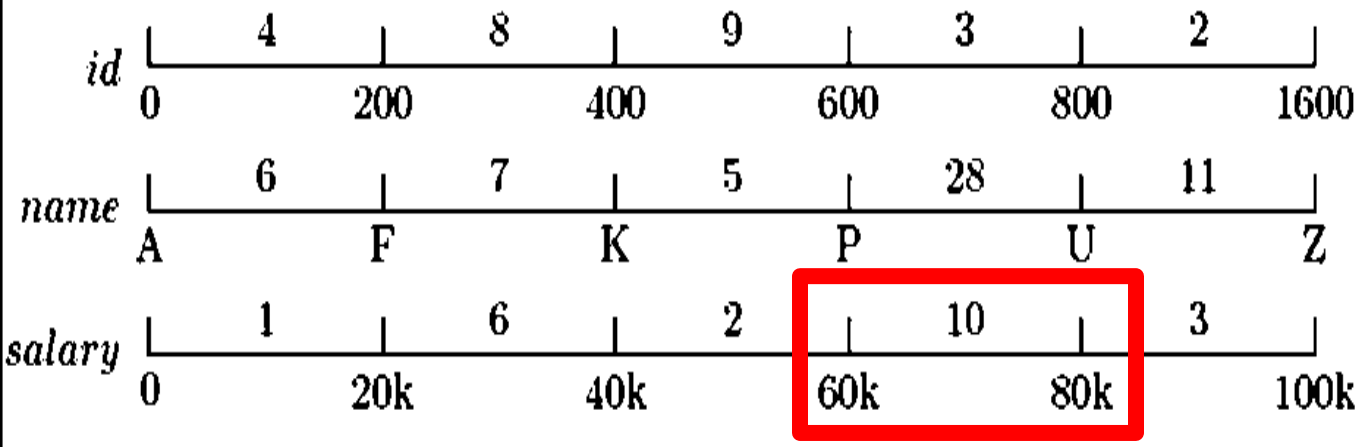
SELECT Name FROM EMP WHERE Salary > 60000 $\rightarrow$ $Salary^S = 3$

فرادداده

نقاط ضعف:

- نشت اطلاعات در مورد داده
  - شاخص‌گذاری امن (secure indexing)
- امکان تولید سطر اضافی در جواب
  - نیاز به پالایش پس از رمزگشایی
- محدودیت

Id	Name	Salary
23	Tom	70000
860	Mary	60000
320	Tony	50000
875	Jerry	5600

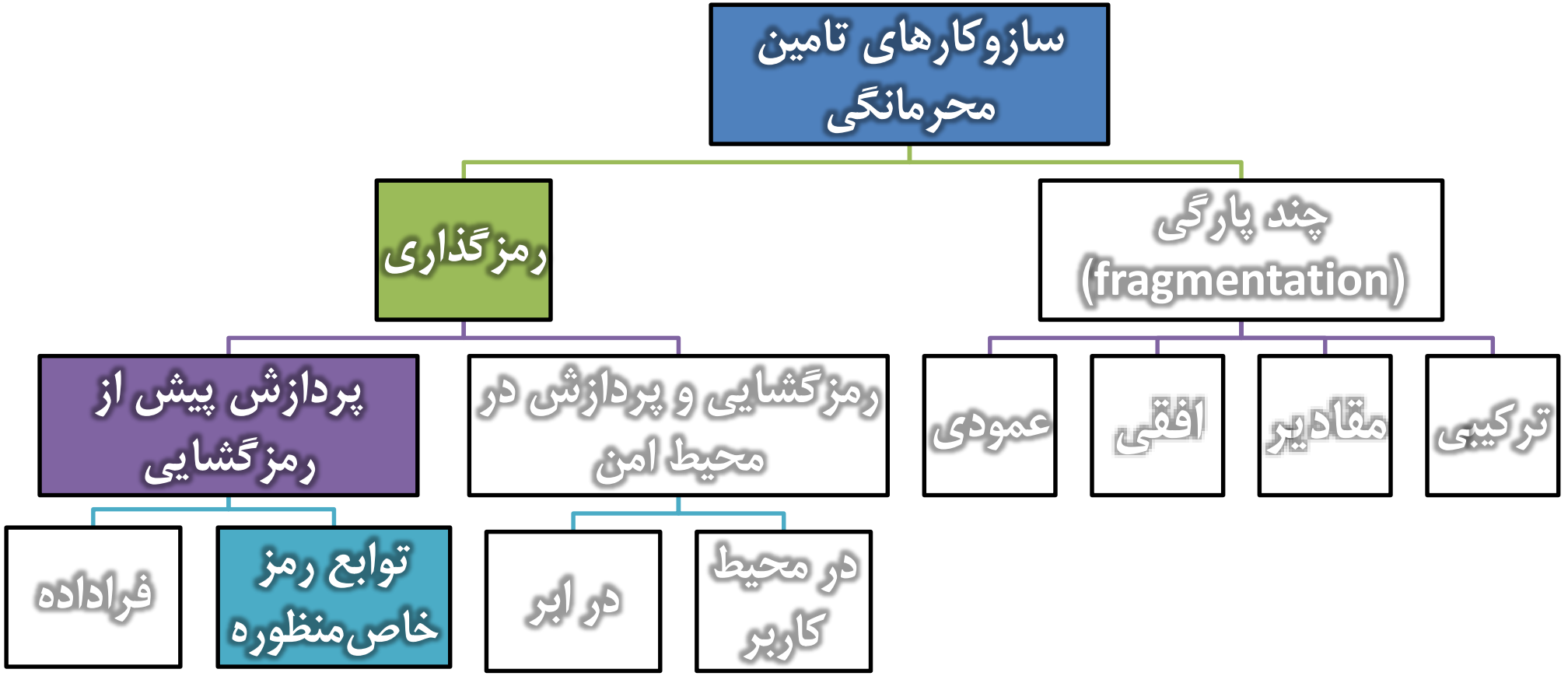


Enc-tuple	Id^S	$Name^S$	$Salary^S$
010011...	4	28	10
110010...	2	5	10
001110...	8	28	2
100011...	2	7	1

SELECT Name FROM t1 WHERE Salary > 65000

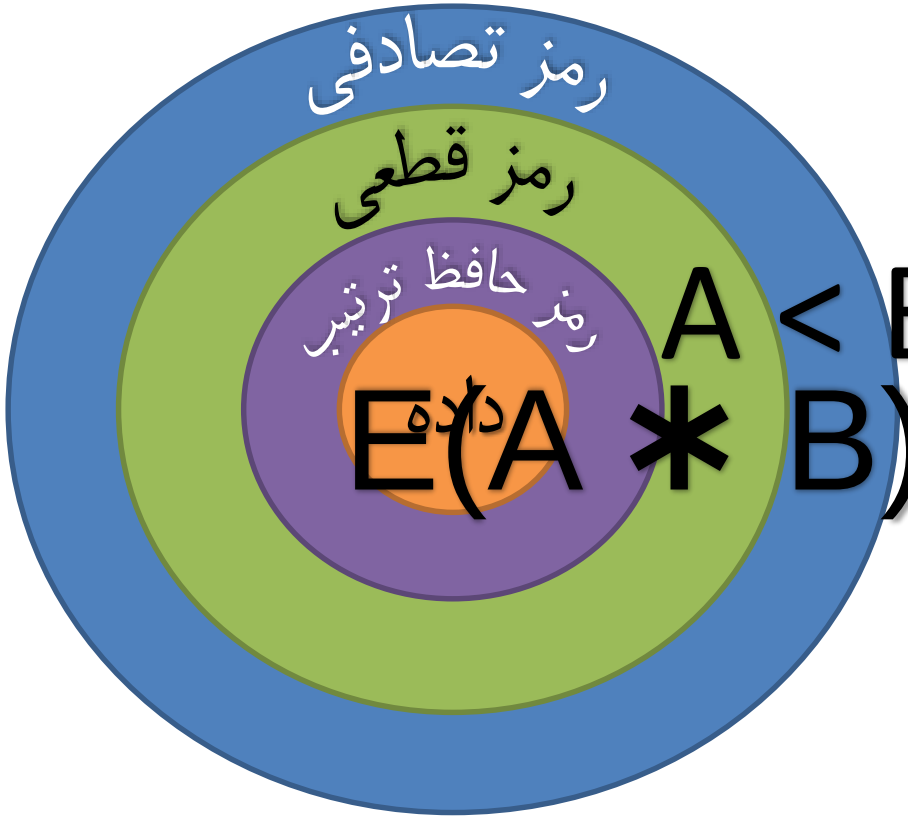
SELECT Name FROM t1 WHERE $Salary^S$ = 10 OR $Salary^S$ = 3

رویکردهای تأمین محرمانگی



رمزگذاری داده

- استفاده از رمزگذاری تمام همریخت (fully homomorphic)
  - سربار زیاد و عدم کارایی در عمل
- استفاده از رمزگذاری‌های خاص منظوره
  - قطعی
  - حافظ ترتیب
  - همریخت جزئی (partial homomorphic)
  - عملیات رشته‌ای (searchable encryption و...)
- رمزگذاری لایه‌ای (پیازی)
  - نیاز به مدیریت لایه‌ها بسته به نوع پرسمان
  - جزئیات در ارائه‌های بعدی ...



$$A \overset{?}{=} B \quad A < B \Leftrightarrow E(A) < E(B) \quad E(A * B) = E(A) \Diamond E(B) \quad A \overset{?}{>=<} B$$

رمزگذاری داده

محدودیت‌ها

- کندی رمزهای خاص‌منظوره
- تنوع عملگرهای تعریف شده در رمز همریخت
- تبدیل انواع
  - اعداد صحیح و اعشاری
- عملیات خاص منظوره
  - LIKE
  - اعمال مربوط به تاریخ
  - ...
- تبدیل یک ستون به چندین ستون
  - محدودتر شدن پرسمان‌های مورد پشتیبانی
- ناگزیر به انجام پالایش اضافی پس از رمزگشایی

A	B	C
1	1	1
2	2	2
3	3	3

SELECT city FROM table1 WHERE city LIKE %r_%

SELECT * FROM table1 WHERE date BETWEEN 1/1/13 AND 2/2/14

SELECT * FROM table1 WHERE A+B>C

رمزگذاری داده

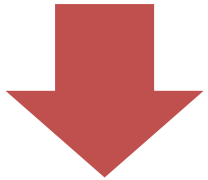
راه حل‌ها

- استفاده از رمزهای سریع در کنار رمزهای خاص منظوره
  - مشابه شاخص (index) ولی با امنیت (و دقت) بالاتر
- تقسیم‌بندی عملیات و انجام حداکثر قسمتهای ممکن در سمت

A (AES)	A (OPE)	A (HOM)
335ABE2…	O(1)	H(1)
A4B56E2…	O(2)	H(2)

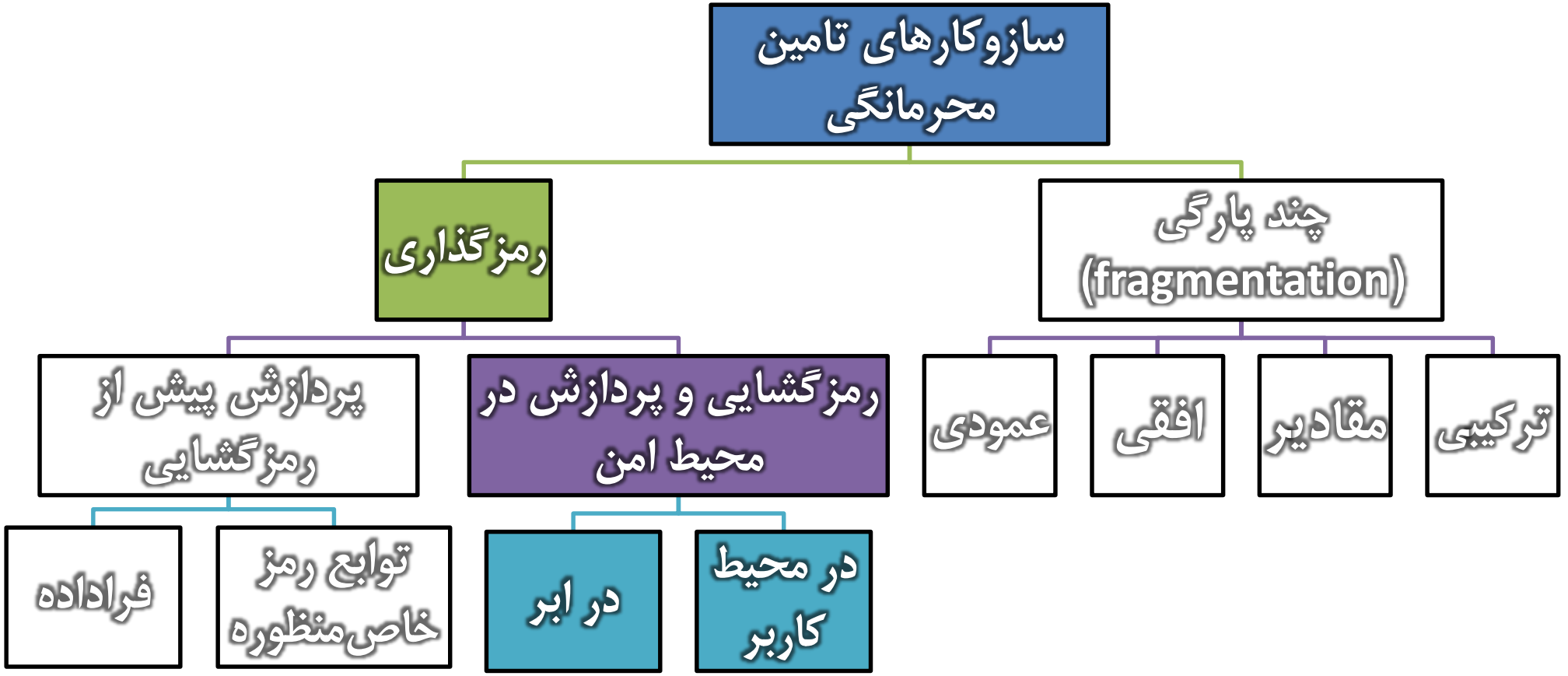
A	B	x	C
1	1	2	1
2	2	4	2
3	3	6	3

```
SELECT * FROM table1 WHERE A+B>C
```



```
SELECT A,B,C FROM
  (SELECT A,B,A+B AS x ,C FROM table1)
WHERE x>C
```

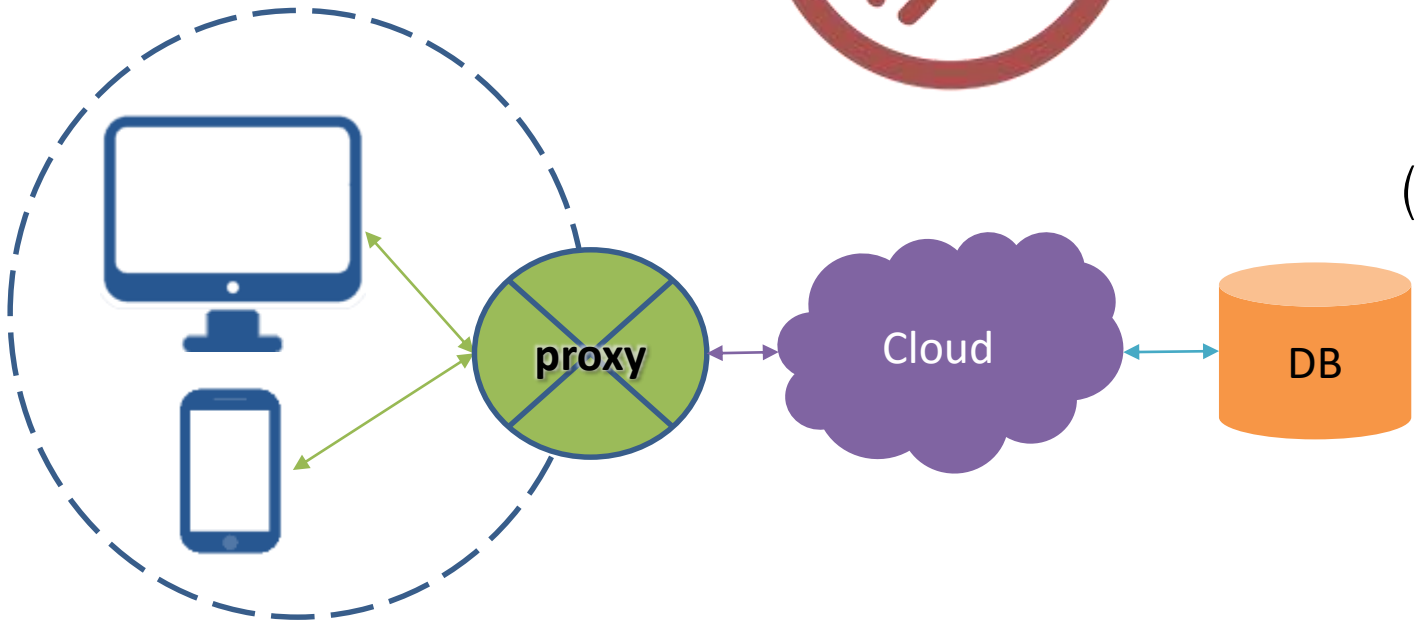
رویکردهای تأمین محرمانگی



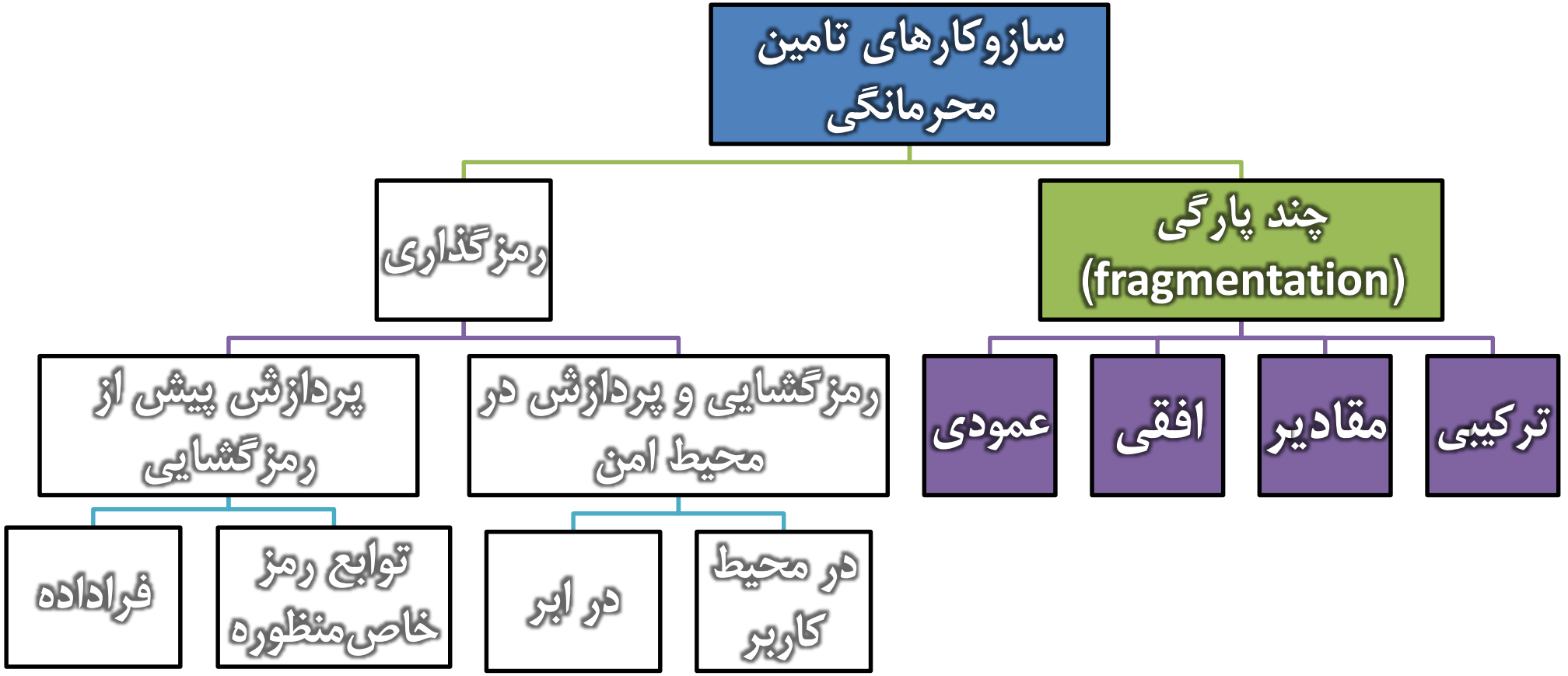
رمزگشایی و پردازش در محیط امن

- در ابر
  - سخت‌افزارهای ضد دستکاری (Tamper-proof hardwares)

- سمت کاربر
  - مبتنی بر پیشکار (proxy)



رویکردهای تأمین محرمانگی



چندپارگی داده (data fragmentation)

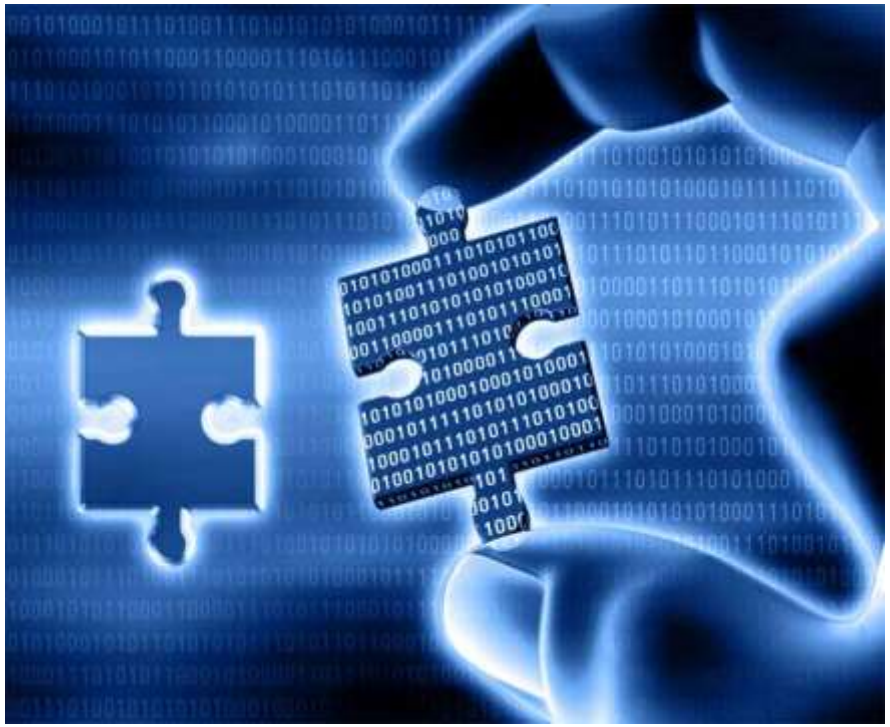
- تقسیم داده بین کارگزاران مختلف
  - محرمانگی ارتباطات بین داده‌ها
  - عدم فاش شدن کل داده‌ها در صورت نشت از یک کارگزار
  - روش‌های تسهیم راز (secret sharing)

id	name	city
2	Al	Teh
3	Nas	Shi
1	Ram	Tab
0	Jav	Ras
2	Ahm	Zab

id	name	city
3	i	Ran
3	er	Raz
8	in	Riz
1	ad	Ht
0	ad	ol

جمع‌بندی

- مزایای برون‌سپاری پایگاه داده
  - کاهش هزینه‌ها
  - دسترس‌پذیری
- چالش‌ها
  - تأمین محرمانگی
  - تضمین جامعیت
  - کنترل دسترسی
  - کارایی
  - وسعت پشتیبانی
- حوزه‌ای پویا و نیازمند راهکارهای جدید برای پوشش خلأهای موجود



با تشکر از توجه شما