مروری بر محصولات موجود در زمینه برون سپاری امن داده

جواد قره چمنی

دانشکده کامپیوتر– دانشگاه صنعتی شریف

gharehchamani@ce.sharif.edu

پژوهشکده پارسا شریف

بیان مسئله

بررسی چند محصول تجاری

بررسی محصولات آزمایشگاهی موجود

امنیت داده در رایانش ابری
رمزگذاری جستجوپذیر متقارن
رمزگذاری جستجوپذیر نامتقارن
رمزگذاری تمام همریخت
برون‌سپاری امن پایگاه داده و رویکردهای تامین محرمانگی
وارسی صحت پاسخ پرسمان روی پایگاه داده برون‌سپاری شده
روشهای ذخیره سازی داده های رمز شده غیر تکراری در ابر
مروری بر محصولات موجود در زمینه برون‌سپاری امن داده
امنیت داده و مدیریت خطردر رایانش ابری

بیان صورت مسئله

امنیت داده در رایانش ابری
رمزگذاری جستجوپذیر متقارن
رمزگذاری جستجوپذیر نامتقارن
رمزگذاری تمام همریخت
برون‌سپاری امن پایگاه داده و رویکردهای تامین محرمانگی
وارسی صحت پاسخ پرسمان روی پایگاه داده برون‌سپاری شده
روشهای ذخیره سازی داده های رمز شده غیر تکراری در ابر
مروری بر محصولات موجود در زمینه برون‌سپاری امن داده
امنیت داده و مدیریت خطردر رایانش ابری

بیان صورت مسئله

امنیت داده در رایانش ابری
رمزگذاری جستجوپذیر متقارن
رمزگذاری جستجوپذیر نامتقارن
رمزگذاری تمام همریخت
برون‌سپاری امن پایگاه داده و رویکردهای تامین محرمانگی
وارسی صحت پاسخ پرسمان روی پایگاه داده برون‌سپاری شده
روشهای ذخیره سازی داده های رمز شده غیر تکراری در ابر
مروری بر محصولات موجود در زمینه برون‌سپاری امن داده
امنیت داده و مدیریت خطردر رایانش ابری

محصولات تجاری موجود در حوزه برون سپاری داده

- Amazon Aurora

- Always Encrypted SQL Server

امنیت داده در رایانش ابری
رمزگذاری جستجوپذیر متقارن
رمزگذاری جستجوپذیر نامتقارن
رمزگذاری تمام همریخت
برون‌سپاری امن پایگاه داده و رویکردهای تامین محرمانگی
وارسی صحت پاسخ پرسمان روی پایگاه داده برون‌سپاری شده
روشهای ذخیره سازی داده های رمز شده غیر تکراری در ابر
مروری بر محصولات موجود در زمینه برون‌سپاری امن داده
امنیت داده و مدیریت خطردر رایانش ابری

امنیت در Amazon Aurora

- ایزوله بودن شبکه با Amazon Virtual Private Cloud

- مجوز دهی در سطح منابع با اتصال به مکانیزم احراز هویت آمازون

- رمزنگاری AES256 برای انتقال

امنیت داده در رایانش ابری
رمزگذاری جستجوپذیر متقارن
رمزگذاری جستجوپذیر نامتقارن
رمزگذاری تمام همریخت
برون‌سپاری امن پایگاه داده و رویکردهای تامین محرمانگی
وارسی صحت پاسخ پرسمان روی پایگاه داده برون‌سپاری شده
روشهای ذخیره سازی داده های رمز شده غیر تکراری در ابر
مروری بر محصولات موجود در زمینه برون‌سپاری امن داده
امنیت داده و مدیریت خطردر رایانش ابری

امنیت Always Encrypted SQL Server

- مشخصات کلی
  - پشتیبانی در MS SQL Server 2016
  - پشتیبانی در Azure SQL Server
  - قابل ترکیب با Transparent Data Encryption

- احراز هویت و مجاز شماری
  - ایجاد Master Key
  - ایجاد Column Encryption Key

- رمزنگاری
  - تنها دو روش قطعی و تصادفی

امنیت داده در رایانش ابری
رمزگذاری جستجوپذیر متقارن
رمزگذاری جستجوپذیر نامتقارن
رمزگذاری تمام همریخت
برون‌سپاری امن پایگاه داده و رویکردهای تامین محرمانگی
وارسی صحت پاسخ پرسمان روی پایگاه داده برون‌سپاری شده
روشهای ذخیره سازی داده های رمز شده غیر تکراری در ابر
مروری بر محصولات موجود در زمینه برون‌سپاری امن داده
امنیت داده و مدیریت خطردر رایانش ابری

محصولات آزمایشگاهی موجود

- (MIT 2012) CryptDB
- (MIT 2013) MONOMI
- (Hong Kong 2015) SDB

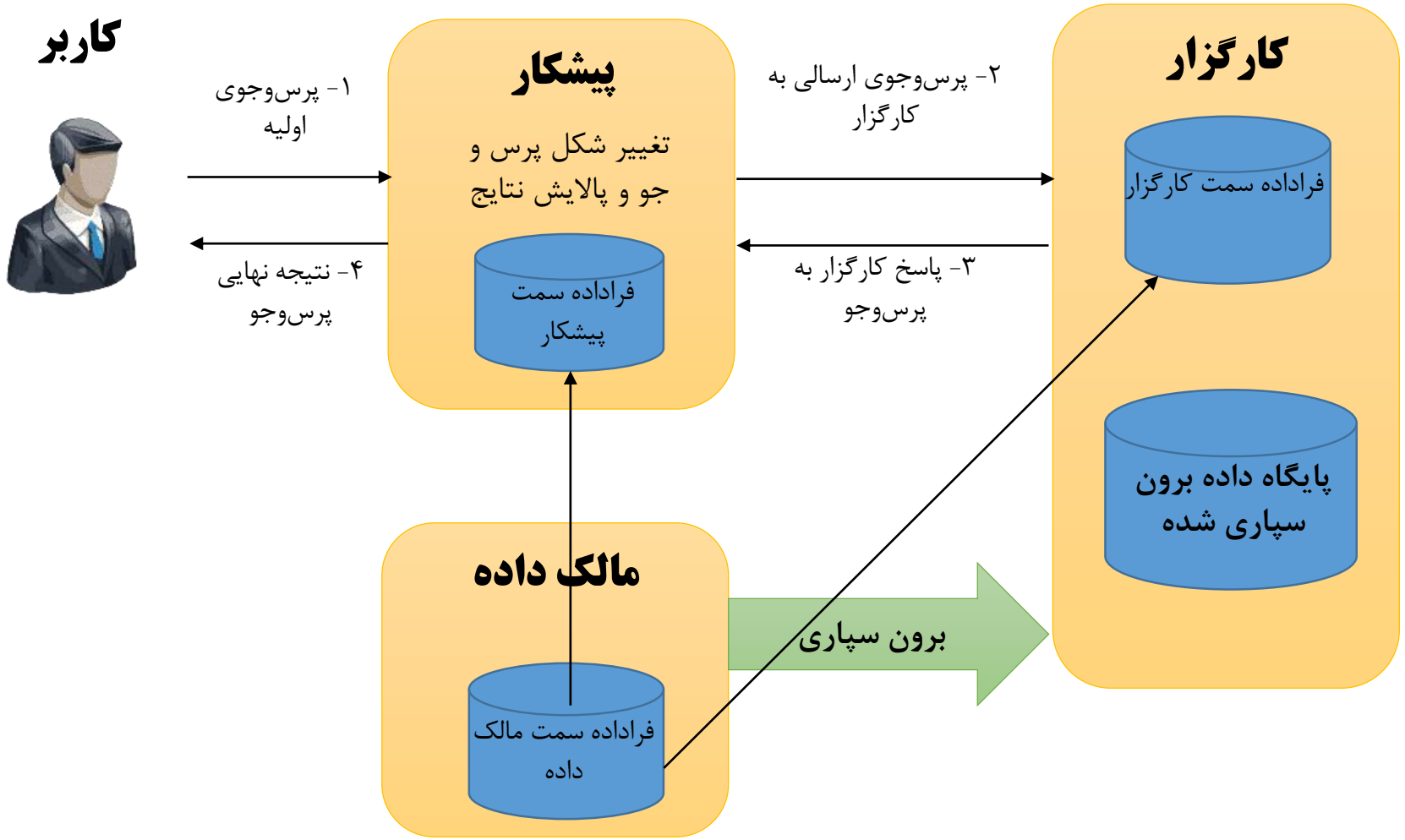

Raluca Popa


Stephen Tu


Zhian He

امنیت داده در رایانش ابری
رمزگذاری جستجوپذیر متقارن
رمزگذاری جستجوپذیر نامتقارن
رمزگذاری تمام همریخت
برون‌سپاری امن پایگاه داده و رویکردهای تامین محرمانگی
وارسی صحت پاسخ پرسمان روی پایگاه داده برون‌سپاری شده
روشهای ذخیره سازی داده های رمز شده غیر تکراری در ابر
مروری بر محصولات موجود در زمینه برون‌سپاری امن داده
امنیت داده و مدیریت خطردر رایانش ابری

معماری مشترک سیستم های برون سپاری



امنیت داده در رایانش ابری
رمزگذاری جستجوپذیر متقارن
رمزگذاری جستجوپذیر نامتقارن
رمزگذاری تمام همریخت
برون‌سپاری امن پایگاه داده و رویکردهای تامین محرمانگی
وارسی صحت پاسخ پرسمان روی پایگاه داده برون‌سپاری شده
روشهای ذخیره سازی داده های رمز شده غیر تکراری در ابر
مروری بر محصولات موجود در زمینه برون‌سپاری امن داده
امنیت داده و مدیریت خطردر رایانش ابری

اهداف در سامانه های برون سپاری

- افزایش حداکثری توان پردازشی
  - پردازش در کارگزار

- افزایش حداکثری توان ذخیره سازی
  - عدم ذخیره سازی در پیشکار

- کاهش هزینه نگهداری

- عدم کاهش امنیت داده ها
  - عدم نمایش داده در کارگزار

امنیت داده در رایانش ابری
رمزگذاری جستجوپذیر متقارن
رمزگذاری جستجوپذیر نامتقارن
رمزگذاری تمام همریخت
برون‌سپاری امن پایگاه داده و رویکردهای تامین محرمانگی
وارسی صحت پاسخ پرسمان روی پایگاه داده برون‌سپاری شده
روشهای ذخیره سازی داده های رمز شده غیر تکراری در ابر
مروری بر محصولات موجود در زمینه برون‌سپاری امن داده
امنیت داده و مدیریت خطردر رایانش ابری

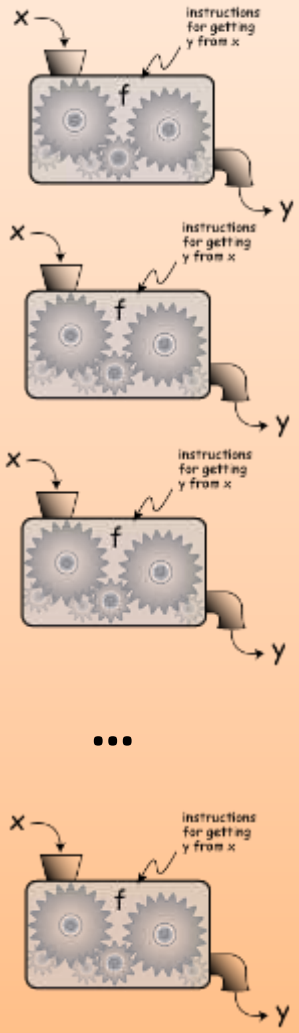
مسئله اصلی!

امنیت داده در رایانش ابری
رمزگذاری جستجوپذیر متقارن
رمزگذاری جستجوپذیر نامتقارن
رمزگذاری تمام همریخت
برون‌سپاری امن پایگاه داده و رویکردهای تامین محرمانگی
وارسی صحت پاسخ پرسمان روی پایگاه داده برون‌سپاری شده
روشهای ذخیره سازی داده های رمز شده غیر تکراری در ابر
مروری بر محصولات موجود در زمینه برون‌سپاری امن داده
امنیت داده و مدیریت خطردر رایانش ابری

CryptDB – اجزای اصلی

امنیت داده در رایانش ابری
رمزگذاری جستجوپذیر متقارن
رمزگذاری جستجوپذیر نامتقارن
رمزگذاری تمام همریخت
برون‌سپاری امن پایگاه داده و رویکردهای تامین محرمانگی
وارسی صحت پاسخ پرسمان روی پایگاه داده برون‌سپاری شده
روشهای ذخیره سازی داده های رمز شده غیر تکراری در ابر
مروری بر محصولات موجود در زمینه برون‌سپاری امن داده
امنیت داده و مدیریت خطردر رایانش ابری

پایگاه داده سمت کارگزار

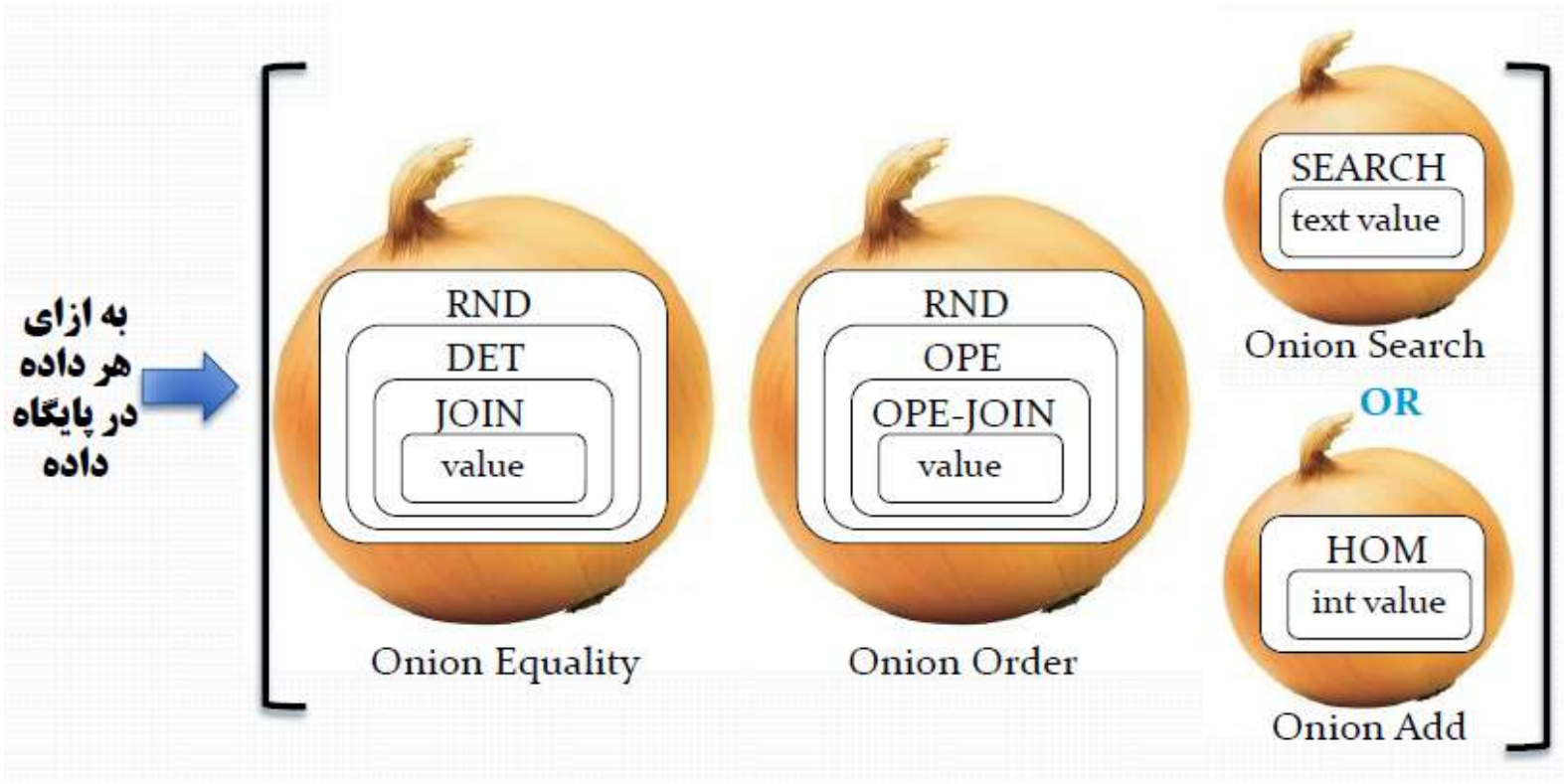


پرس و جوی بازنویسی شده

پروکسی کارگزار (مغز اصلی)

پرس و جوی خام

CryptDB – نحوه ذخیره سازی داده ها



امنیت داده در رایانش ابری
رمزگذاری جستجوپذیر متقارن
رمزگذاری جستجوپذیر نامتقارن
رمزگذاری تمام همریخت
برون‌سپاری امن پایگاه داده و رویکردهای تامین محرمانگی
وارسی صحت پاسخ پرسمان روی پایگاه داده برون‌سپاری شده
روشهای ذخیره سازی داده های رمز شده غیر تکراری در ابر
مروری بر محصولات موجود در زمینه برون‌سپاری امن داده
امنیت داده و مدیریت خطردر رایانش ابری

CryptDB – نحوه اجرای پرس و جو

SELECT ID FROM Employees
WHERE Name = 'Alice'

پاسخ
رمزگشایی شده

UPDATE Table1 SET C2-Eq =
DECRYPT_RND(Key,T1.C2,C2-IV)
Table1 WHERE C2-Eq = x7b3d

پاسخ رمز شده

امنیت داده در رایانش ابری
رمزگذاری جستجوپذیر متقارن
رمزگذاری جستجوپذیر نامتقارن
رمزگذاری تمام همریخت
برون‌سپاری امن پایگاه داده و رویکردهای تامین محرمانگی
وارسی صحت پاسخ پرسمان روی پایگاه داده برون‌سپاری شده
روشهای ذخیره سازی داده های رمز شده غیر تکراری در ابر
مروری بر محصولات موجود در زمینه برون‌سپاری امن داده
امنیت داده و مدیریت خطردر رایانش ابری

مشکلات CryptDB

- عدم پشتیبانی از پرس و جو های تو در تو ۴/۲۲

```
USE [AdventureWorks2014];
GO

SELECT  [Name]
FROM    [Production].[Product]
WHERE   [ListPrice] = ( SELECT  [ListPrice]
                        FROM    [Production].[Product]
                        WHERE   [Name] = 'Chain Stays'
                      );
GO
```

- تنها پشتیبانی از انواع داده عددی و رشته ای

- نیاز به هوش انسانی برای مدیریت پرس و جو های پیچیده

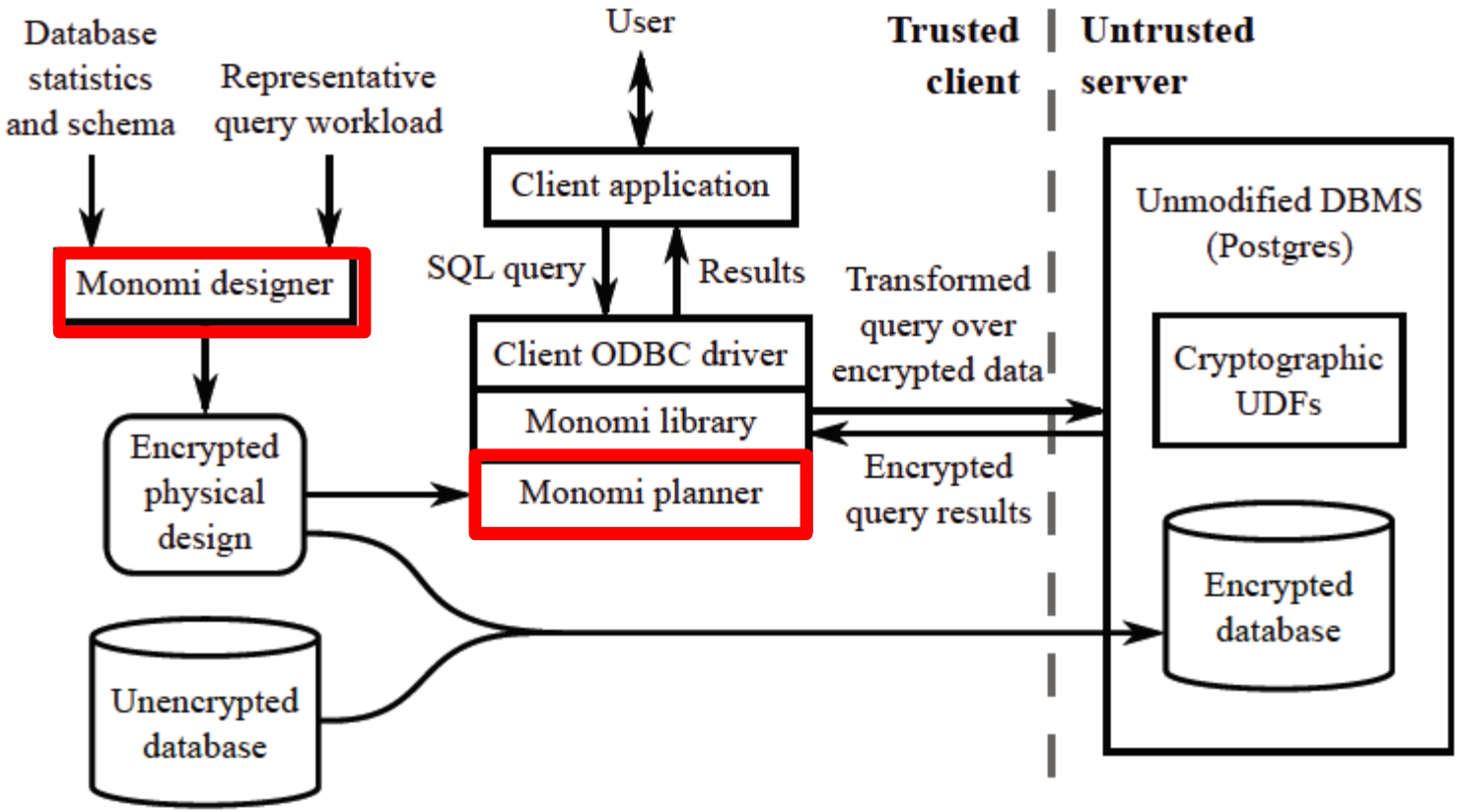
امنیت داده در رایانش ابری
رمزگذاری جستجوپذیر متقارن
رمزگذاری جستجوپذیر نامتقارن
رمزگذاری تمام همریخت
برون‌سپاری امن پایگاه داده و رویکردهای تامین محرمانگی
وارسی صحت پاسخ پرسمان روی پایگاه داده برون‌سپاری شده
روشهای ذخیره سازی داده های رمز شده غیر تکراری در ابر
مروری بر محصولات موجود در زمینه برون‌سپاری امن داده
امنیت داده و مدیریت خطردر رایانش ابری

MONOMI

- انتقال داده های میانی به پیشکار موجب کندی سیستم
- محاسبات پیچیده روی داده های رمز شده هزینه بر
  - FHE ها 10^9 بار کند تر
  - روش های تک منظوره مناسب تر ولی سخت تر
- افزودن ستون اضافه موجب افزایش سرعت برخی و کاهش سایرین
- ارایه راهکاری بر مبنای CryptDB و پیاده سازی Planner و Designer
- پشتیبانی ۱۹/۲۲ مدل پرس و جوی TPC-H
- هدف پشتیبانی پرس و جوهای تحلیلی

امنیت داده در رایانش ابری
رمزگذاری جستجوپذیر متقارن
رمزگذاری جستجوپذیر نامتقارن
رمزگذاری تمام همریخت
برون‌سپاری امن پایگاه داده و رویکردهای تامین محرمانگی
وارسی صحت پاسخ پرسمان روی پایگاه داده برون‌سپاری شده
روشهای ذخیره سازی داده های رمز شده غیر تکراری در ابر
مروری بر محصولات موجود در زمینه برون‌سپاری امن داده
امنیت داده و مدیریت خطردر رایانش ابری

MONOMI – معماری کلی



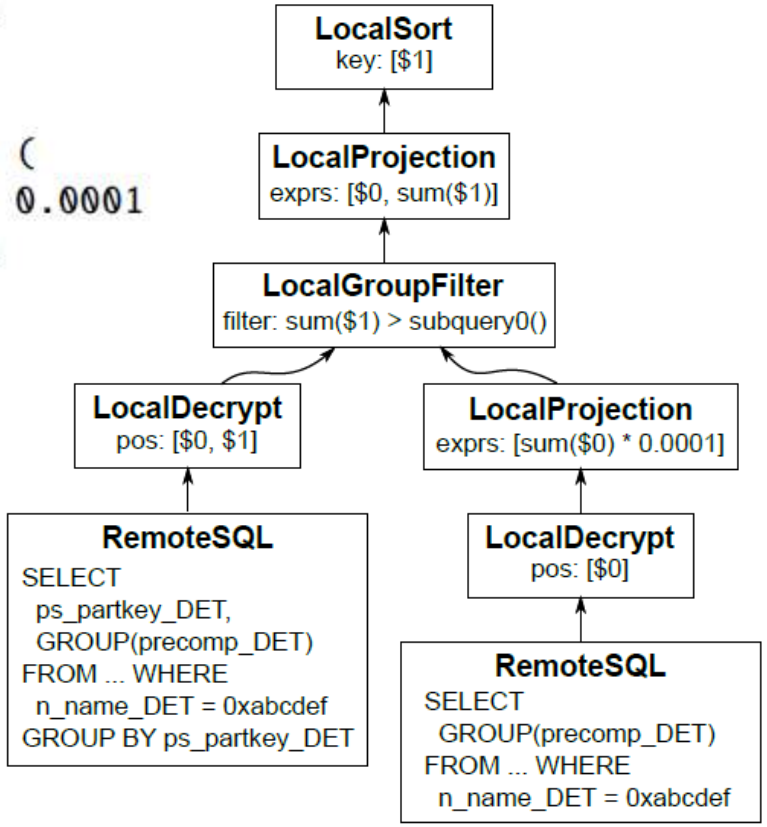
S. Tu, M. F. Kaashoek, S. Madden, and N. Zeldovich, "Processing analytical queries over encrypted data," in *Proceedings of the VLDB Endowment*, 2013, vol. 6, no. 5, pp. 289–300.

امنیت داده در رایانش ابری
رمزگذاری جستجوپذیر متقارن
رمزگذاری جستجوپذیر نامتقارن
رمزگذاری تمام همریخت
برون‌سپاری امن پایگاه داده و رویکردهای تامین محرمانگی
وارسی صحت پاسخ پرسمان روی پایگاه داده برون‌سپاری شده
روشهای ذخیره سازی داده های رمز شده غیر تکراری در ابر
مروری بر محصولات موجود در زمینه برون‌سپاری امن داده
امنیت داده و مدیریت خطردر رایانش ابری

Planner & Designer – MONOMI

- عدم امکان کل پرس و جو در کارگزار

```
SELECT   ps_partkey,
         SUM(ps_supplycost * ps_availqty) AS value
FROM     partsupp JOIN supplier JOIN nation
WHERE    n_name = :1
GROUP BY ps_partkey
HAVING   SUM(ps_supplycost * ps_availqty) > (
  SELECT SUM(ps_supplycost * ps_availqty) * 0.0001
  FROM   partsupp JOIN supplier JOIN nation
  WHERE  n_name = :1 )
ORDER BY value DESC;
```



S. Tu, M. F. Kaashoek, S. Madden, and N. Zeldovich, "Processing analytical queries over encrypted data," in *Proceedings of the VLDB Endowment*, 2013, vol. 6, no. 5, pp. 289–300.

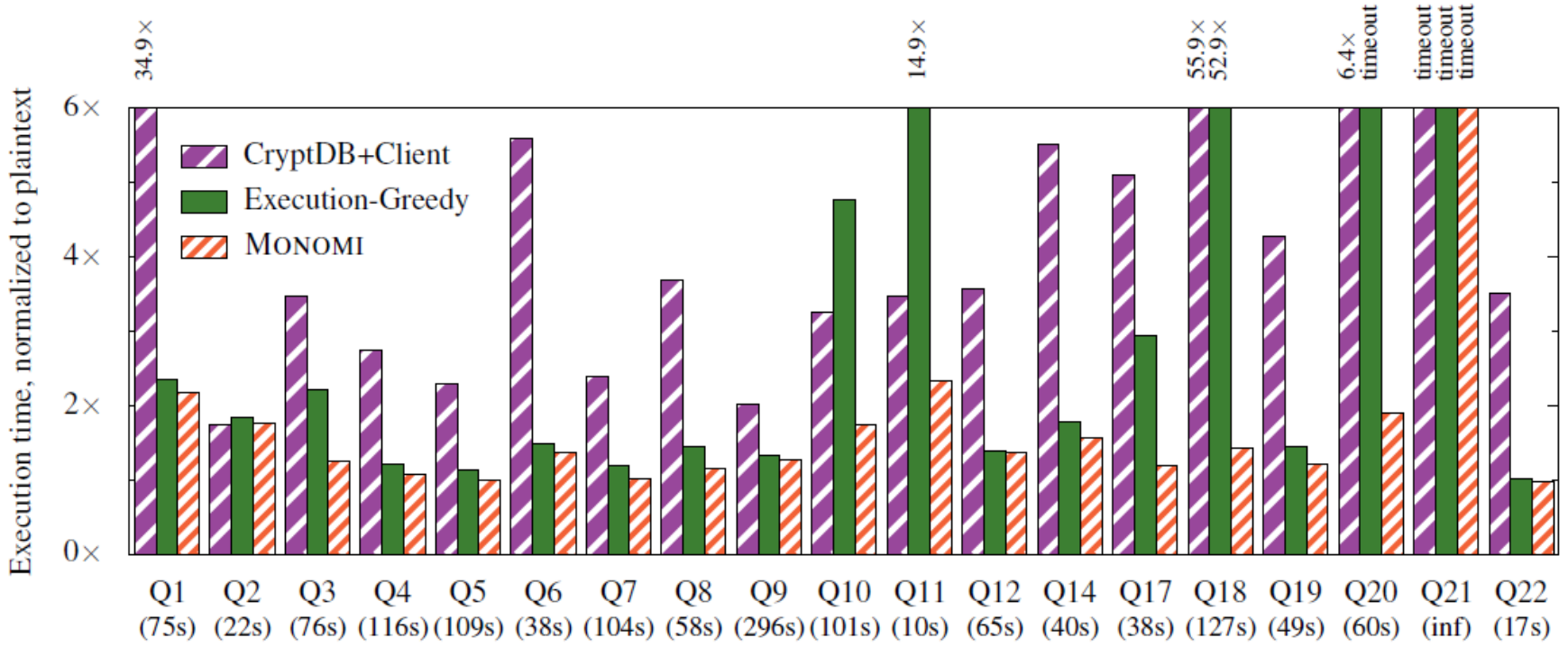
امنیت داده در رایانش ابری
رمزگذاری جستجوپذیر متقارن
رمزگذاری جستجوپذیر نامتقارن
رمزگذاری تمام همریخت
برون‌سپاری امن پایگاه داده و رویکردهای تامین محرمانگی
وارسی صحت پاسخ پرسمان روی پایگاه داده برون‌سپاری شده
روشهای ذخیره سازی داده های رمز شده غیر تکراری در ابر
مروری بر محصولات موجود در زمینه برون‌سپاری امن داده
امنیت داده و مدیریت خطردر رایانش ابری

MONOMI– راه کارهایی جهت بهبود کارایی

- محاسبه و ذخیره از پیش انجام شده به ازای هر سطر
  - ps_supplycost * ps_availqty
- رمزنگاری با سربار کم حافظه
  - استفاده از مد هایی از AES که حجم داده رمز شده خیلی تغییر نکند
  - ذخیره سال از تاریخ در یک ستون دیگر
- ذخیره مقادیر رمز همریخت جمعی Pailliar برخی ستون ها برای انجام عملیات ریاضی
- استفاده از designer جهت یافتن بهترین ساختار

امنیت داده در رایانش ابری
رمزگذاری جستجوپذیر متقارن
رمزگذاری جستجوپذیر نامتقارن
رمزگذاری تمام همریخت
برون‌سپاری امن پایگاه داده و رویکردهای تامین محرمانگی
وارسی صحت پاسخ پرسمان روی پایگاه داده برون‌سپاری شده
روشهای ذخیره سازی داده های رمز شده غیر تکراری در ابر
مروری بر محصولات موجود در زمینه برون‌سپاری امن داده
امنیت داده و مدیریت خطردر رایانش ابری

MONOMI– نتایج ارزیابی



S. Tu, M. F. Kaashoek, S. Madden, and N. Zeldovich, "Processing analytical queries over encrypted data," in *Proceedings of the VLDB Endowment*, 2013, vol. 6, no. 5, pp. 289–300.

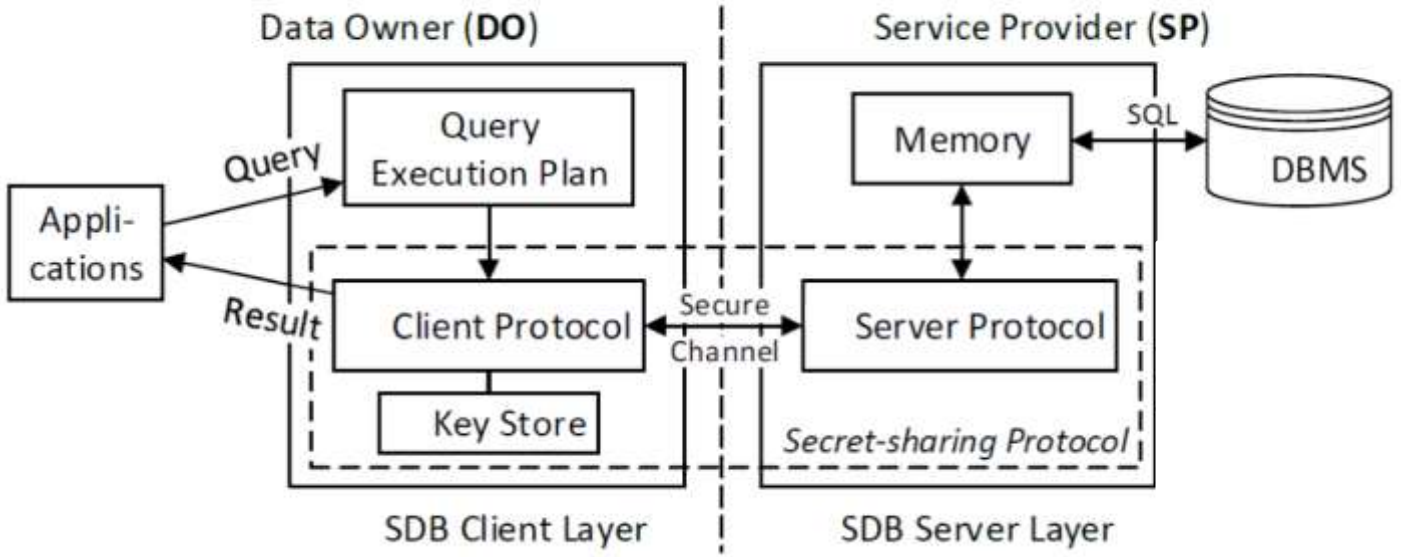
امنیت داده در رایانش ابری
رمزگذاری جستجوپذیر متقارن
رمزگذاری جستجوپذیر نامتقارن
رمزگذاری تمام همریخت
برون‌سپاری امن پایگاه داده و رویکردهای تامین محرمانگی
وارسی صحت پاسخ پرسمان روی پایگاه داده برون‌سپاری شده
روشهای ذخیره سازی داده های رمز شده غیر تکراری در ابر
مروری بر محصولات موجود در زمینه برون‌سپاری امن داده
امنیت داده و مدیریت خطردر رایانش ابری

SDB

- استفاده از نقش مالک داده جهت پردازش برخی قسمت ها
- **ارایه اپراتورهای بهینه و قابل ترکیب**
- امکان استفاده از اپراتور ها برای داده های رمز شده و غیر رمز شده
- امکان اعمال روی هر نوع پایگاه داده
- ارایه اثبات برای امنیت شمای رمزنگاری آن
- بر مبنای تسهیم راز
- **تنها بر روی داده های عددی قابل اعمال**

امنیت داده در رایانش ابری
رمزگذاری جستجوپذیر متقارن
رمزگذاری جستجوپذیر نامتقارن
رمزگذاری تمام همریخت
برون‌سپاری امن پایگاه داده و رویکردهای تامین محرمانگی
وارسی صحت پاسخ پرسمان روی پایگاه داده برون‌سپاری شده
روشهای ذخیره سازی داده های رمز شده غیر تکراری در ابر
مروری بر محصولات موجود در زمینه برون‌سپاری امن داده
امنیت داده و مدیریت خطردر رایانش ابری

SDB – معماری کلی



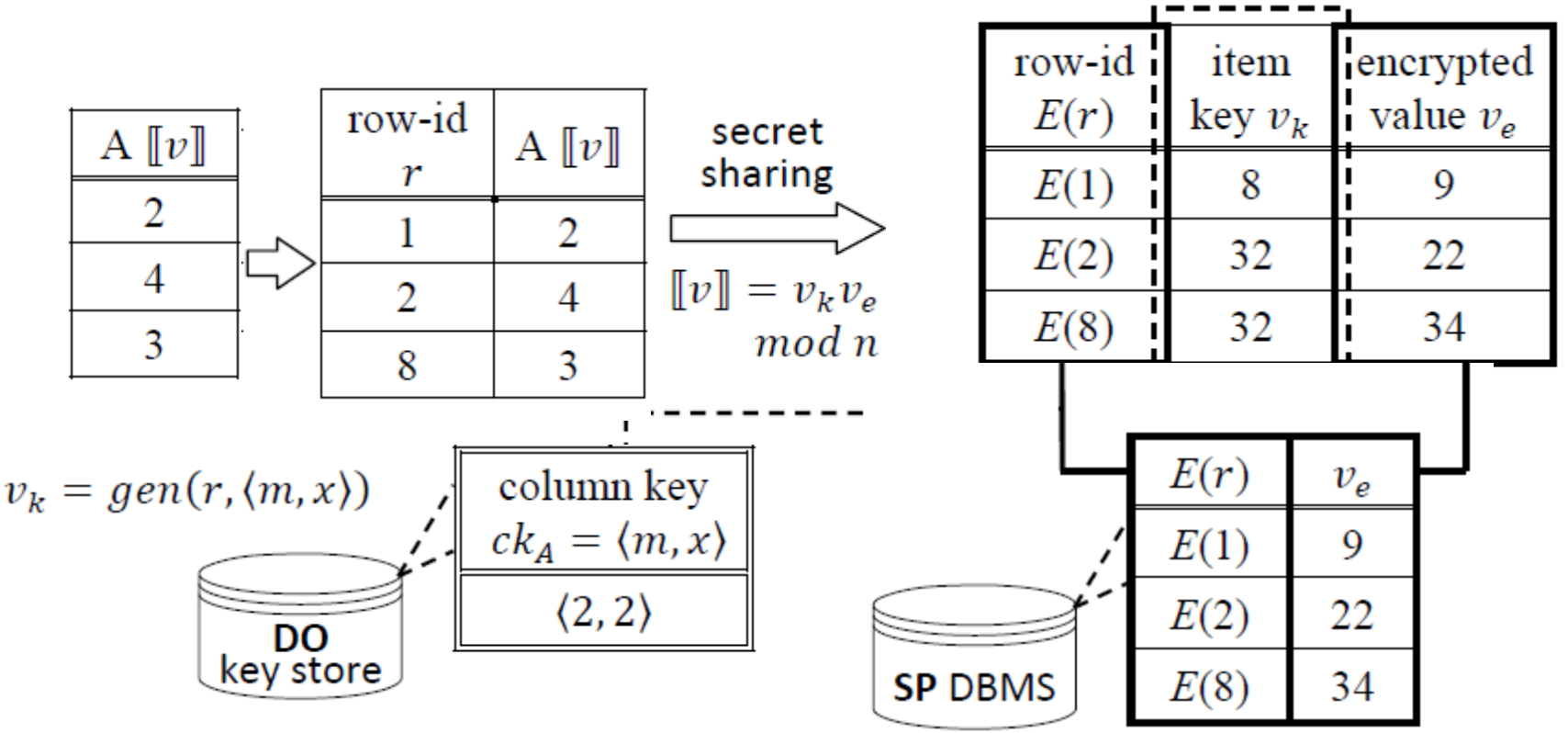
Z. He, W. K. Wong, B. Kao, D. W. L. Cheung, R. Li, S. M. Yiu, and E. Lo, "SDB: a secure query processing system with data interoperability," *Proc. VLDB Endow.*, vol. 8, no. 12, pp. 1876–1879, 2015.

امنیت داده در رایانش ابری
رمزگذاری جستجوپذیر متقارن
رمزگذاری جستجوپذیر نامتقارن
رمزگذاری تمام همریخت
برون‌سپاری امن پایگاه داده و رویکردهای تامین محرمانگی
وارسی صحت پاسخ پرسمان روی پایگاه داده برون‌سپاری شده
روشهای ذخیره سازی داده های رمز شده غیر تکراری در ابر
مروری بر محصولات موجود در زمینه برون‌سپاری امن داده
امنیت داده و مدیریت خطردر رایانش ابری

SDB– نحوه رمز کردن داده ها

$$v_k = gen(r, \langle m, x \rangle) = mg^{(rx \bmod \phi(n))} \bmod n. \qquad v_e = \mathcal{E}([\![v]\!], v_k) = [\![v]\!] v_k^{-1} \bmod n,$$

$$(g = 2,\ n = 35)$$



Z. He, W. K. Wong, B. Kao, D. W. L. Cheung, R. Li, S. M. Yiu, and E. Lo, "SDB: a secure query processing system with data interoperability," *Proc. VLDB Endow.*, vol. 8, no. 12, pp. 1876–1879, 2015.

امنیت داده در رایانش ابری
رمزگذاری جستجوپذیر متقارن
رمزگذاری جستجوپذیر نامتقارن
رمزگذاری تمام همریخت
برون‌سپاری امن پایگاه داده و رویکردهای تامین محرمانگی
وارسی صحت پاسخ پرسمان روی پایگاه داده برون‌سپاری شده
روشهای ذخیره سازی داده های رمز شده غیر تکراری در ابر
مروری بر محصولات موجود در زمینه برون‌سپاری امن داده
امنیت داده و مدیریت خطردر رایانش ابری

SDB– نحوه پیاده سازی ضرب کردن

$$C = A \times B \ (g = 2,\ n = 35)$$

Plaintext values

A	B
2	3
4	1

C = A X B

C
6
4

$$c_e = a_e \cdot b_e$$

DO

ck_A = <2, 2>
ck_B = <1, 3>

ck_C = <2, 5>

$$ck_C = \langle m_C, x_C \rangle = \langle m_A m_B, x_A + x_B \rangle$$

SP

E(r)	A_e	B_e
E(1)	9	31
E(2)	22	29

C_e
34
8

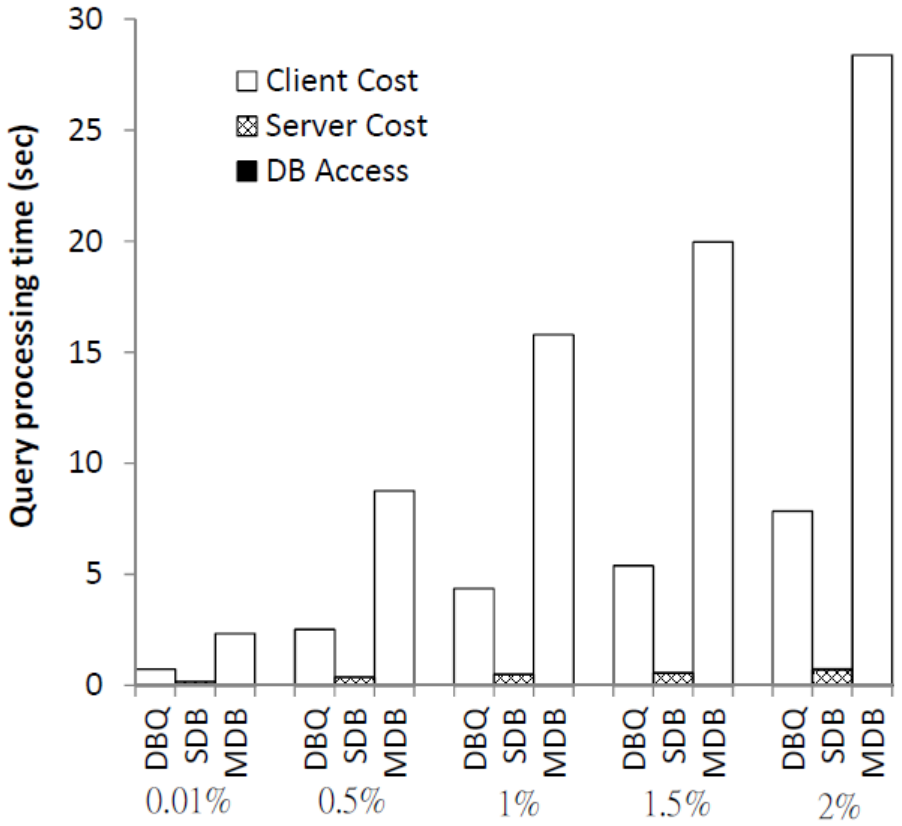
$$c_k = m_C \cdot g^{r x_C} = m_A \cdot m_B \cdot g^{r(x_A + x_B)} = a_k b_k \pmod n$$

$$[\![c]\!] = c_e c_k = a_e b_e c_k = [\![a]\!] a_k^{-1} [\![b]\!] b_k^{-1} a_k b_k = [\![a]\!][\![b]\!]$$

Z. He, W. K. Wong, B. Kao, D. W. L. Cheung, R. Li, S. M. Yiu, and E. Lo, “SDB: a secure query processing system with data interoperability,” *Proc. VLDB Endow.*, vol. 8, no. 12, pp. 1876–1879, 2015.

امنیت داده در رایانش ابری
رمزگذاری جستجوپذیر متقارن
رمزگذاری جستجوپذیر نامتقارن
رمزگذاری تمام همریخت
برون‌سپاری امن پایگاه داده و رویکردهای تامین محرمانگی
وارسی صحت پاسخ پرسمان روی پایگاه داده برون‌سپاری شده
روشهای ذخیره سازی داده های رمز شده غیر تکراری در ابر
مروری بر محصولات موجود در زمینه برون‌سپاری امن داده
امنیت داده و مدیریت خطردر رایانش ابری

مقایسه کارایی



Z. He, W. K. Wong, B. Kao, D. W. L. Cheung, R. Li, S. M. Yiu, and E. Lo, "SDB: a secure query processing system with data interoperability," *Proc. VLDB Endow.*, vol. 8, no. 12, pp. 1876–1879, 2015.

امنیت داده در رایانش ابری
رمزگذاری جستجوپذیر متقارن
رمزگذاری جستجوپذیر نامتقارن
رمزگذاری تمام همریخت
برون‌سپاری امن پایگاه داده و رویکردهای تامین محرمانگی
وارسی صحت پاسخ پرسمان روی پایگاه داده برون‌سپاری شده
روشهای ذخیره سازی داده های رمز شده غیر تکراری در ابر
مروری بر محصولات موجود در زمینه برون‌سپاری امن داده
امنیت داده و مدیریت خطردر رایانش ابری

جمع بندی

- فعلا نمی توان از توابع FHE برای ایجاد رمزنگاری کاربردی استفاده کرد
- لازم است از توابع خاص منظوره استفاده کرد
- برای ایجاد قابلیت اجرای پرس و جو های پیچیده نیاز به وجود Planner است
- برای تامین امنیت، داده خام نباید وارد/ خارج کارگزار شود
- باید تا جای ممکن پردازش ها را در سمت کارگزار قرار داد تا از منابع آن استفاده کرد
- **نیاز به یک محصول امن و کارای برون سپاری در حوزه تجاری و تحقیقاتی وجود دارد**

امنیت داده در رایانش ابری
رمزگذاری جستجوپذیر متقارن
رمزگذاری جستجوپذیر نامتقارن
رمزگذاری تمام همریخت
برون‌سپاری امن پایگاه داده و رویکردهای تامین محرمانگی
وارسی صحت پاسخ پرسمان روی پایگاه داده برون‌سپاری شده
روشهای ذخیره سازی داده های رمز شده غیر تکراری در ابر
مروری بر محصولات موجود در زمینه برون‌سپاری امن داده
امنیت داده و مدیریت خطردر رایانش ابری

ارجاعات

- https://azure.microsoft.com/en-us/documentation/articles/sql-database-security/
- http://aws.amazon.com/rds/aurora/details/#security
- R. A. Popa, C. Redfield, N. Zeldovich, and H. Balakrishnan, “CryptDB: Processing queries on an encrypted database,” *Commun. ACM*, vol. 55, no. 9, pp. 103–111, 2012.
- S. Tu, M. F. Kaashoek, S. Madden, and N. Zeldovich, “Processing analytical queries over encrypted data,” in *Proceedings of the VLDB Endowment*, 2013, vol. 6, no. 5, pp. 289–300.
- W. K. Wong, B. Kao, D. W. L. Cheung, R. Li, and S. M. Yiu, “Secure query processing with data interoperability in a cloud database environment,” *Proc. 2014 ACM SIGMOD Int. Conf. Manag. data - SIGMOD ’14*, pp. 1395–1406, 2014.
- Z. He, W. K. Wong, B. Kao, D. W. L. Cheung, R. Li, S. M. Yiu, and E. Lo, “SDB: a secure query processing system with data interoperability,” *Proc. VLDB Endow.*, vol. 8, no. 12, pp. 1876–1879, 2015.
- V. Gadepally, B. Hancock, B. Kaiser, J. Kepner, P. Michaleas, M. Varia, and A. Yerukhimovich, “Computing on Masked Data to improve the Security of Big Data,” 2015.
- .....

امنیت داده در رایانش ابری
رمزگذاری جستجوپذیر متقارن
رمزگذاری جستجوپذیر نامتقارن
رمزگذاری تمام همریخت
برون‌سپاری امن پایگاه داده و رویکردهای تامین محرمانگی
وارسی صحت پاسخ پرسمان روی پایگاه داده برون‌سپاری شده
روشهای ذخیره سازی داده های رمز شده غیر تکراری در ابر
مروری بر محصولات موجود در زمینه برون‌سپاری امن داده
امنیت داده و مدیریت خطردر رایانش ابری

امنیت داده در رایانش ابری
رمزنگاری جستجوپذیر متقارن
رمزنگاری جستجوپذیر نامتقارن
رمزگذاری تمام همریخت
برون‌سپاری امن پایگاه داده و رویکردهای تامین محرمانگی
وارسی صحت پاسخ پرسمان روی پایگاه داده برون‌سپاری شده
روشهای ذخیره سازی داده های رمز شده غیر تکراری در ابر
مروری بر محصولات موجود در زمینه برون‌سپاری امن داده
امنیت داده و مدیریت خطردر رایانش ابری

با تشکر از توجه شما