



انجمن رمز ایران



قطب علمی رمز



Open Community of Cloud Computing
جامعه آزاد رایانش ابری ایران



مرکز تحقیقات رایانش ابری

کارگاه عملی امنیت داده و مدیریت مخاطرات در رایانش ابری

مرتضی سرگلزایی جوان

مسئول مرکز تحقیقات رایانش ابری
موسس جامعه آزاد رایانش ابری ایران

www.msjavaan.ir

[@msjavaan_ir](https://www.instagram.com/msjavaan_ir)

چشم‌انداز

□ مقدمه

- مروری بر رایانش ابری با مثال‌های عملی
- خدمات رایانش ابری در ایران

□ مدیریت مخاطرات

- مفاهیم پایه و چهارچوب ارزیابی
- مطالعه موردی (کارگاه عملی)

□ نتیجه‌گیری

- بده‌بستان امنیت و کارایی
- نمایش نهایی!

امنیت داده در رایانش ابری

رمزگذاری جستجوپذیر متقارن

رمزگذاری جستجوپذیر نامتقارن

رمزگذاری تمام‌همریخت

برون‌سپاری امن پایگاه داده و

رویکردهای تامین محرمانگی

وارسی صحت پاسخ پرسمان روی

پایگاه داده برون‌سپاری شده

روشهای ذخیره‌سازی داده‌های

رمز شده غیر تکراری در ابر

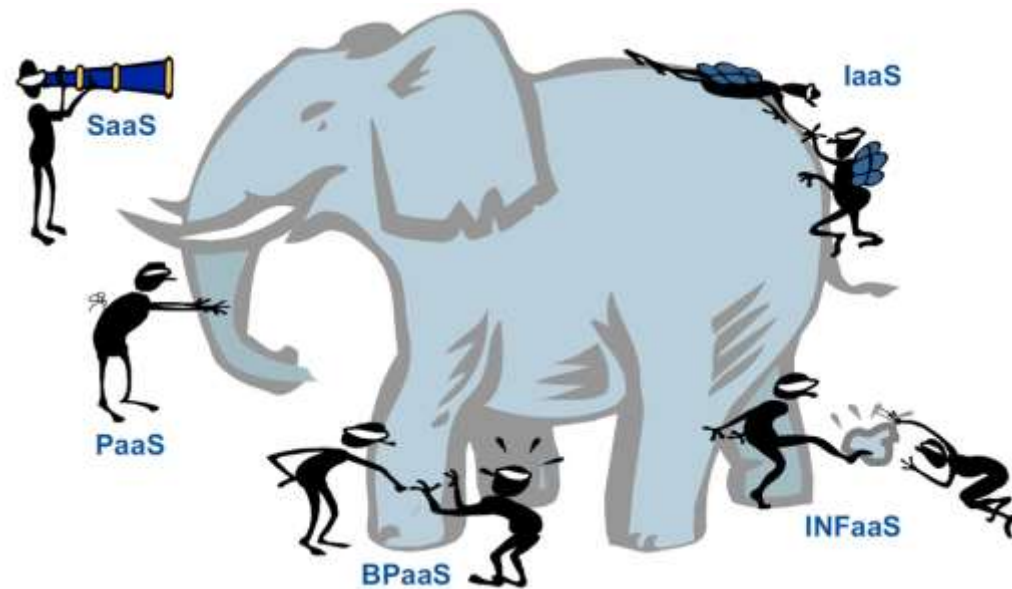
مروری بر محصولات موجود

در زمینه برون‌سپاری امن داده

امنیت داده و مدیریت مخاطرات

در رایانش ابری

مقدمه



امنیت داده در رایانش ابری

رمز گذاری جستجوپذیر متقارن

رمز گذاری جستجوپذیر نامتقارن

رمز گذاری تمام همریخت

برون سپاری امن پایگاه داده و رویکردهای تامین محرمانگی

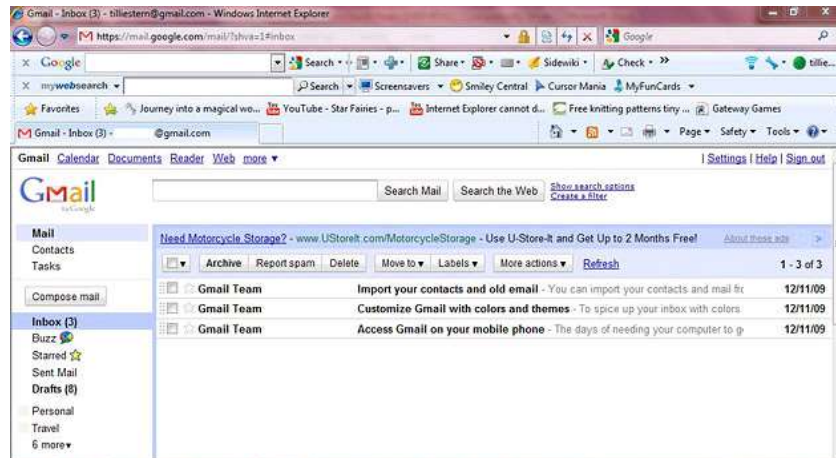
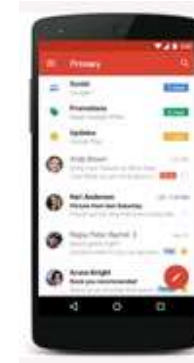
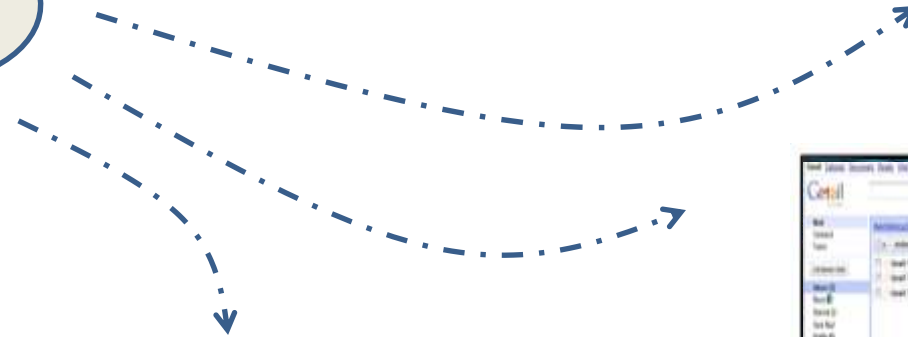
وارسی صحت پاسخ پرسمان روی پایگاه داده برون سپاری شده

روشهای ذخیره سازی داده های رمز شده غیر تکراری در ابر

مروری بر محصولات موجود در زمینه برون سپاری امن داده

امنیت داده و مدیریت مخاطرات در رایانش ابری

مثال موردی : Email



امنیت داده در رایانش ابری

رمز گذاری جستجوپذیر نامتقارن

رمز گذاری جستجوپذیر نامتقارن

رمز گذاری تمام هم ریخت

برون سپاری امن پایگاه داده و رویکردهای تامین محرمانگی

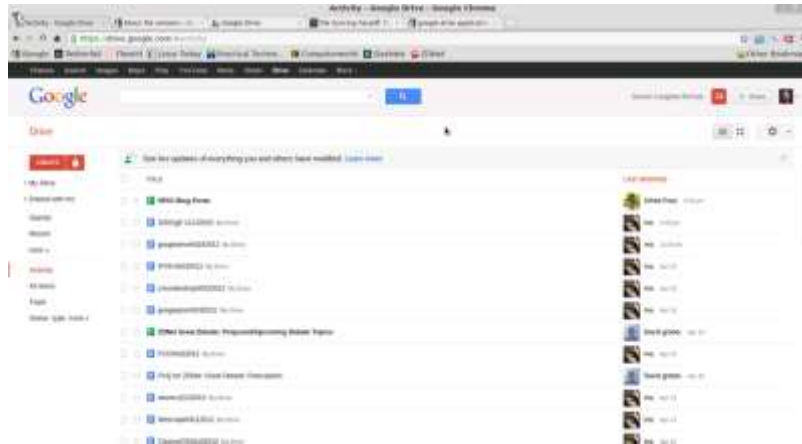
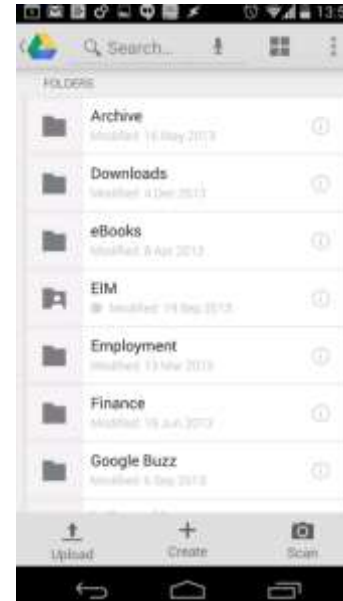
وارسی صحت پاسخ پرسمان روی پایگاه داده برون سپاری شده

روشهای ذخیره سازی داده های رمز شده غیر تکراری در ابر

مروری بر محصولات موجود در زمینه برون سپاری امن داده

امنیت داده و مدیریت مخاطرات در رایانش ابری

مثال موردی : Drive



امنیت داده در رایانش ابری

رمز گذاری جستجوپذیر متقارن

رمز گذاری جستجوپذیر نامتقارن

رمز گذاری تمام هم ریخت

برون سپاری امن پایگاه داده و

رویکردهای تامین محرمانگی

وارسی صحت پاسخ پرسمان روی

پایگاه داده برون سپاری شده

روشهای ذخیره سازی داده های

رمز شده غیر تکراری در ابر

مروری بر محصولات موجود

در زمینه برون سپاری امن داده

امنیت داده و مدیریت مخاطرات

در رایانش ابری

مثال موردی : Office



امنیت داده در رایانش ابری

رمز گذاری جستجوپذیر متقارن

رمز گذاری جستجوپذیر نامتقارن

رمز گذاری تمام هم ریخت

برون سپاری امن پایگاه داده و رویکردهای تامین محرمانگی

وارسی صحت پاسخ پرسمان روی پایگاه داده برون سپاری شده

روشهای ذخیره سازی داده های رمز شده غیر تکراری در ابر

مروری بر محصولات موجود در زمینه برون سپاری امن داده

امنیت داده و مدیریت مخاطرات در رایانش ابری

زیست بوم رایانش ابری در ایران: taxonomy.occc.ir

امنیت داده در رایانش ابری

رمز گذاری جستجوپذیر متقارن

رمز گذاری جستجوپذیر نامتقارن

رمز گذاری تمام هم ریخت

برون سپاری امن پایگاه داده و

رویکردهای تامین محرمانگی

وارسی صحت پاسخ پرمسمن روی

پایگاه داده برون سپاری شده

روشهای ذخیره سازی داده های

رمز شده غیر تکراری در ابر

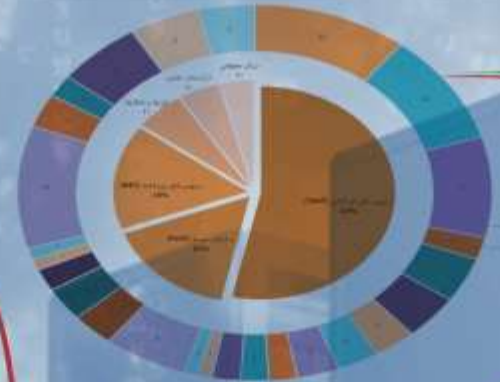
مروری بر محصولات موجود

در زمینه برون سپاری امن داده

امنیت داده و مدیریت مخاطرات

در رایانش ابری

تاکسونومی رایانش ابری در ایران



- سرویس های مالی
- سرویس های آموزشی
- سرویس های فارسی
- سرویس های آموزشی
- سازگاری
- ایمنی
- تجارت الکترونیک
- سازگاری
- ایمنی
- تجارت الکترونیک
- سازگاری
- ایمنی
- تجارت الکترونیک

خدمات مالی اغلب نرم افزارهای شخصی ارائه می شوند و امکان تحلیل محتاج در آنها و بازها و پرداخت ها را فراهم می کنند. در بعضی موارد امکان انجام برنامه ریزی های مالی نیز برای کاربران فراهم است.

نرم افزارهای ارائه خدمات آموزشی بیشترین توزیع سرویس های نرم افزاری ابری را در ایران به خود اختصاص داده اند. از جمله این خدمات می توان به ایجاد کلاس درس مجازی، مدیریت محتوا، برگزاری دوره های آموزشی، برگزاری آزمون های آنلاین و تصحیح و تحلیل نتایج آنها اشاره کرد.

نرم افزارهای بومی جوینگر از جمله نرم افزارهای رایج در شکل گیری اکوسیستم رایانش ابری داده محور هستند که با ارائه خدمات پایه جستجو در حوزه های تخصصی مختلف، امکان ایجاد فرایندهای تجاری مختلف را فراهم می کنند.

آزمایشگاه های تحقیقاتی در حوزه رایانش ابری و پردازش های فوق سریع (ابر رایانش) خدمات متعددی را در سطح کشور ارائه می دهند و هسته های توسعه علمی این صنعت را در کشور تشکیل می دهند.

شیکه های توزیع محتوا ترکیبی از زیرساخت ها و مکانیزم های هستند که نحوه توزیع محتوا و خدمات اینترنتی به صورت مناسب انجام پذیرفته و کاربران کیفیت بهتری را از وب تجربه کنند.

ارایه خدمات پایه پردازشی نظیر سرویس های مجازی بطور گسترده در جزایر داده کشور (به صورت مستقیم) یا از طریق فروشندگان های واسطه (با ارایه خدمات ارزش افزوده) انجام می شود. پشتیبانی از مدل مدیریت سلف سرویس و رقابت بر سر قیمت و کیفیت از جمله موضوعات رایج در این بخش می باشد.

بسترهای مبتنی و ارایه داده بصورت آزاد تجاری از عوامل محرک در توسعه خدمات داده محور ابری می باشد تا توسعه دهندگان بتوانند از طریق واسطه های دسترسی به داده سرویس های خود را تعدیه کنند و با پردازش آنها خدمات ارزش افزوده این را به کاربران ارایه کنند.

شناسایی و معرفی سرویس های رایانش ابری تولید داخل

اجرای کسب و کارها بر روی ابر و ارایه فرایندی تجاری بصورت ابری به گونه ای که بتوان آنها را با فرایندهای کاری دیگر یکپارچه کرد، از موضوعاتی است که با سرعت زیادی رو به رشد است و تاثیر بسیار زیادی در توسعه با بهره برداری از این صنعت از نظر اقتصادی دارد.



مدیریت رویدادها به صورت برخط



امنیت داده در رایانش ابری

رمز گذاری جستجوپذیر متقارن

رمز گذاری جستجوپذیر نامتقارن

رمز گذاری 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 مخاطرات در رایانش ابری

برگزاری کنفرانس و همایش به صورت برخط

امنیت داده در رایانش ابری

رمز گذاری جستجوپذیر متقارن

رمز گذاری جستجوپذیر نامتقارن

رمز گذاری تمام هم ریخت

برون سپاری امن پایگاه داده و

رویکردهای تامین محرمانگی

وارسی صحت پاسخ پرسمان روی

پایگاه داده برون سپاری شده

روشهای ذخیره سازی داده های

رمز شده غیر تکراری در ابر

مروری بر محصولات موجود

در زمینه برون سپاری امن داده

امنیت داده و مدیریت مخاطرات

در رایانش ابری

The screenshot shows an Adobe Connect meeting window. The main content is a presentation slide titled "Top 20 Software License Misuse and Piracy Hotspots" based on aggregated CodeArmor intelligence data from October 2014. The slide features a world map with numbered hotspots and a list of countries: 1. China, 2. Russia, 3. United States, 4. Ukraine, 5. Taiwan, 6. Italy, 7. France, 8. Mexico, 9. Germany, 10. Turkey, 11. Brazil, 12. India, 13. Hungary, 14. Korea, 15. Romania, 16. Spain, 17. Poland, 18. United Kingdom, 19. Canada, 20. Australia. A large text overlay states "43 % of software being pirated." The slide also includes the e-seminar logo and social media handles. The meeting interface includes a video feed of a male presenter, a chat window, and a toolbar at the bottom.

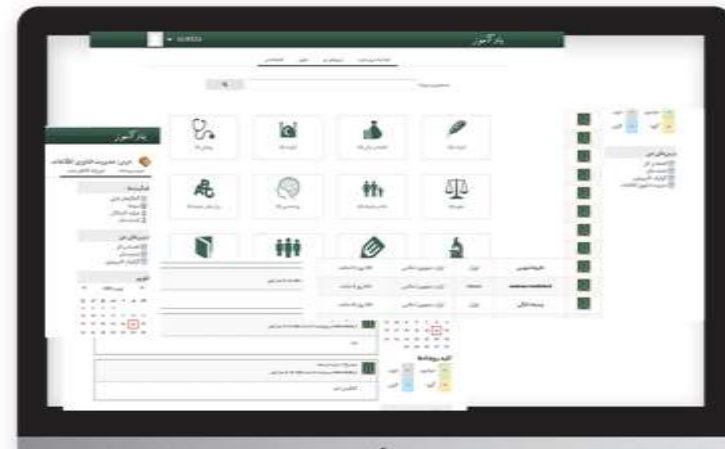
کلاس درس برخط



کلاس درس خود را به اینترنت بیاورید!

اگر در دانشگاه تدریس می کنید، اگر تدریس بسیار درسی هستید، اگر در آموزشگاه، مدرسه و حتی به صورت خصوصی به فعالیت آموزشی میپردازید، با یادآموز، آموزش خود را بهبود بخشید! با استفاده از امکانات ما می توانید راحت تر تدریس کنید!

امکاناتی از قبیل تحویل و دریافت تمرینات و نمرات آن ها از طریق اینترنت، نمره دهی به دانشجویان، پرسش و پاسخ اینترنتی در کلاس، امکان آپلود فایل، عکس و فیلم؛ باعث می شود تا مدیریت کلاس شما بسیار راحت تر، مفیدتر و جذاب تر گردد.



امنیت داده در رایانش ابری

رمز گذاری جستجوپذیر متقارن

رمز گذاری جستجوپذیر نامتقارن

رمز گذاری تمام هم ریخت

برون سپاری امن پایگاه داده و

رویکردهای تامین محرمانگی

وارسی صحت پاسخ پرسمان روی

پایگاه داده برون سپاری شده

روشهای ذخیره سازی داده های

رمز شده غیر تکراری در ابر

مروری بر محصولات موجود

در زمینه برون سپاری امن داده

امنیت داده و مدیریت مخاطرات

در رایانش ابری

سیستم حسابداری شخصی



امنیت داده در رایانش ابری

رمز گذاری جستجوپذیر متقارن

رمز گذاری جستجوپذیر نامتقارن

رمز گذاری تمام هم ریخت

برون سپاری امن پایگاه داده و رویکردهای تامین محرمانگی

وارسی صحت پاسخ پرسمان روی پایگاه داده برون سپاری شده

روشهای ذخیره سازی داده های رمز شده غیر تکراری در ابر

مروری بر محصولات موجود در زمینه برون سپاری امن داده

امنیت داده و مدیریت مخاطرات در رایانش ابری

ارسال فکس بر خط

امنیت داده در رایانش ابری

رمز گذاری جستجوپذیر متقارن

رمز گذاری جستجوپذیر نامتقارن

رمز گذاری تمام هم ریخت

برون سپاری امن پایگاه داده و

رویکردهای تامین محرمانگی

وارسی صحت پاسخ پرسمان روی
پایگاه داده برون سپاری شدهروشهای ذخیره سازی داده های
رمز شده غیر تکراری در ابرمروری بر محصولات موجود
در زمینه برون سپاری امن دادهامنیت داده و مدیریت مخاطرات
در رایانش ابری

آقای مرتضی جوان

FAX.IR

بایگانی | ارسالی

نام فایل	وضعیت	دریافت کننده	تاریخ	هزینه	پادداشت
fax.pdf	موفق	88762037	1393/4/1 10:42	2	
fax.pdf	ناموفقی اشغالی خط مقصد	88762037	1393/4/1 10:33	1	

تایخ در هر صفحه 10

ابزارکار

تنظیمات

راهنما

دریافتی (0)

ارسالی

منتظر ارسال (0)

هزینه نام (1)

داشبورد

ارسال

بایگانی

ارسال مجدد (Resend)

ارسال (Forward)

تغییر نام (Rename)

دریافت (Download)

پیش نمایش (Preview)

امضا (Sign)



ابزارهای توسعه همراه و تارنما

ورود / ثبت نام

آشنایی اهمیت امکانات دمو آموزش قیمت گذاری ارتباط با ما

یوتشه

با پوشه قدرتمند شوید

برای کاربران خود اعلان (پوش نوتیفیکیشن - Push Notification) بفرستید و با آنها در ارتباط باشید

ثبت نام

دموی پوشه



بکتوری نیازهای سمت سرور شما را سریع تر، امن تر و کم هزینه تر فراهم می کند.

مدیریت فایل، وب سرور، مرکز بازی، دیتابیس، سرویس بلادرنگ و کاربران را در هر اندازه، از یک نقطه مدیریت کنید

چرا بکتوری؟

بتل مدیریت

امنیت داده در رایانش ابری

رمز گذاری جستجوپذیر متقارن

رمز گذاری جستجوپذیر نامتقارن

رمز گذاری تمام هم ریخت

برون سپاری امن پایگاه داده و

رویکردهای تامین محرمانگی

وارسی صحت پاسخ پرسمان روی

پایگاه داده برون سپاری شده

روشهای ذخیره سازی داده های

رمز شده غیر تکراری در ابر

مروری بر محصولات موجود

در زمینه برون سپاری امن داده

امنیت داده و مدیریت مخاطرات

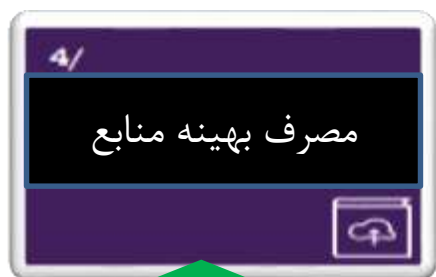
در رایانش ابری

مزایای اتصال به شبکه رایانش ...

تا ۲۰۲۰

۹۴ درصد سازمان ها و شرکت ها
به زیرساخت های ابری متصل می شوند

\$200B

Spent by business on
public cloud services

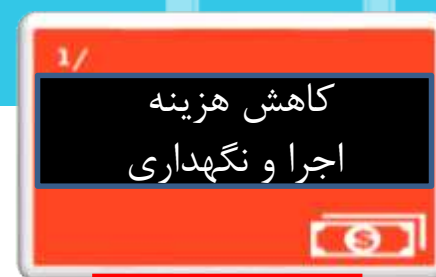
65%



87%



95%



98%

امنیت داده در رایانش ابری

رمز گذاری جستجوپذیر متقارن

رمز گذاری جستجوپذیر نامتقارن

رمز گذاری تمام هم ریخت

برون سپاری امن پایگاه داده و

رویکردهای تامین محرمانگی

وارسی صحت پاسخ پرسمان روی

پایگاه داده برون سپاری شده

روشهای ذخیره سازی داده های

رمز شده غیر تکراری در ابر

مروری بر محصولات موجود

در زمینه برون سپاری امن داده

امنیت داده و مدیریت مخاطرات

در رایانش ابری

مخاطرات استفاده از شبکه های مختلف چیست؟

امنیت داده در رایانش ابری

رمز گذاری جستجوپذیر متقارن

رمز گذاری جستجوپذیر نامتقارن

رمز گذاری تمام هم ریخت

برون سپاری امن پایگاه داده و

رویکردهای تامین محرمانگی

وارسی صحت پاسخ پرسمان روی

پایگاه داده برون سپاری شده

روشهای ذخیره سازی داده های

رمز شده غیر تکراری در ابر

مروری بر محصولات موجود

در زمینه برون سپاری امن داده

امنیت داده و مدیریت مخاطرات

در رایانش ابری



شبکه تلفن

قطع شدن تلفن
شکست مکالمات



شبکه آب

قطع شدن آب
سوراخ شدن لوله آب
استفاده غیر مجاز از انشعاب آب
خشکسالی



شبکه برق

قطع شدن برق
استفاده غیر مجاز از انشعاب برق
اختلال در تجهیزات کنترلی

استفاده از شبکه های همگانی یک ضرورت است... (مخاطرات امنیتی!؟)

طی ۱۵ الی ۲۰ سال آینده، استفاده از فناوری اطلاعات آنچنان فراگیر می شود که اتصال به شبکه رایانش یک نیاز همگانی خواهد بود.



شبکه تلفن



شبکه آب



شبکه برق

امنیت داده در رایانش ابری

رمز گذاری جستجوپذیر متقارن

رمز گذاری جستجوپذیر نامتقارن

رمز گذاری تمام هم ریخت

برون سپاری امن پایگاه داده و

رویکردهای تامین محرمانگی

وارسی صحت پاسخ پرمسان روی

پایگاه داده برون سپاری شده

روشهای ذخیره سازی داده های

رمز شده غیر تکراری در ابر

مروری بر محصولات موجود

در زمینه برون سپاری امن داده

امنیت داده و مدیریت مخاطرات

در رایانش ابری

آیا تا کنون با عدم دسترسی به یک خدمت مواجه شده اید؟

امنیت داده در رایانش ابری

رمز گذاری جستجوپذیر متقارن

رمز گذاری جستجوپذیر نامتقارن

رمز گذاری تمام هم ریخت

برون سپاری امن پایگاه داده و

رویکردهای تامین محرمانگی

وارسی صحت پاسخ پرسمان روی

پایگاه داده برون سپاری شده

روشهای ذخیره سازی داده های

رمز شده غیر تکراری در ابر

مروری بر محصولات موجود

در زمینه برون سپاری امن داده

امنیت داده و مدیریت مخاطرات

در رایانش ابری



The connection has timed out

The server at taskulu.ir is taking too long to respond.

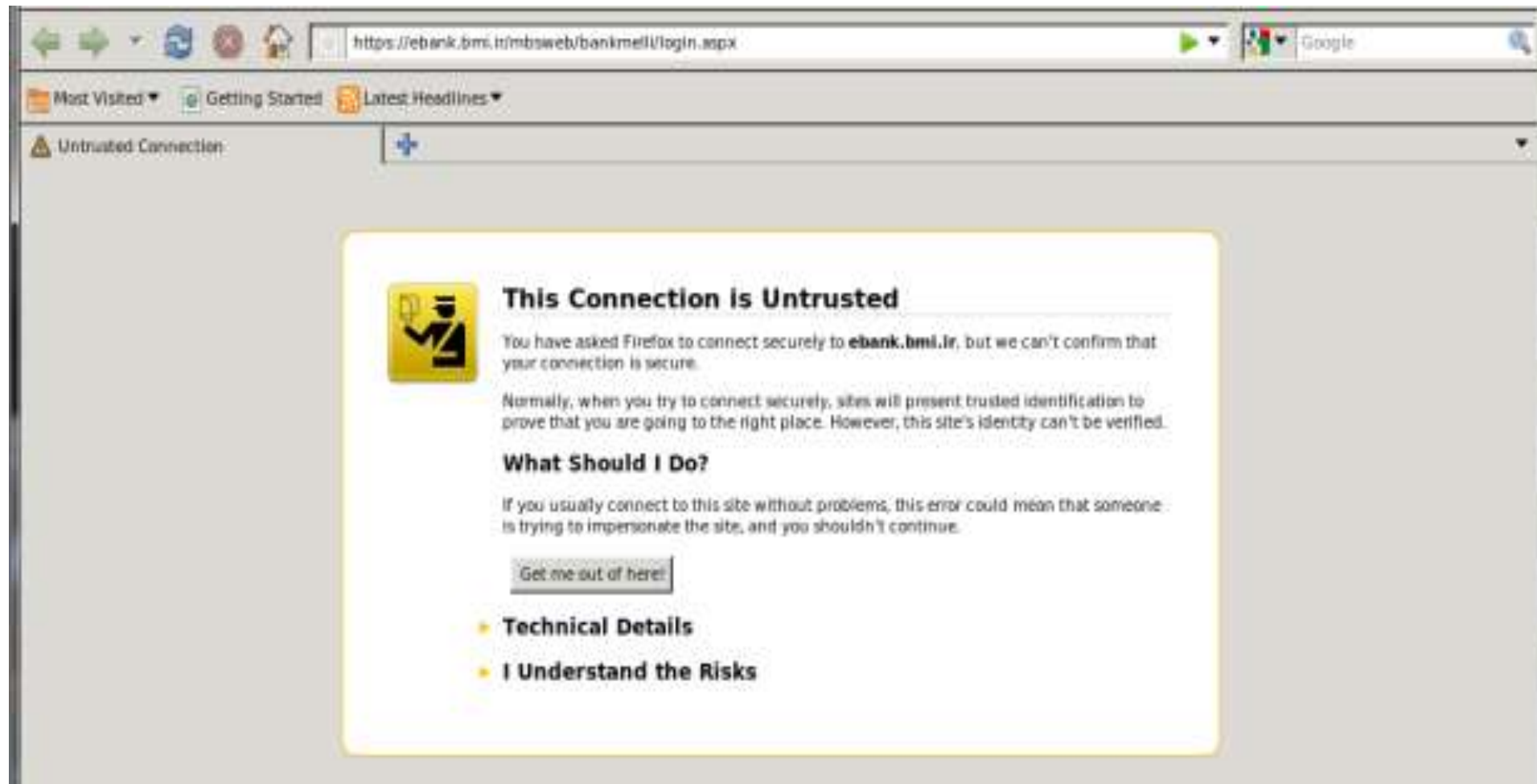
- The site could be temporarily unavailable or too busy. Try again in a few moments.
- If you are unable to load any pages, check your computer's network connection.
- If your computer or network is protected by a firewall or proxy, make sure that Firefox is permitted to access the Web.

Try Again

پرداخت موفقیت آمیز نبود. کد خطا: 131

مشتری گرامی با سلام احتراماً در حال حاضر ارائه سرویس امکان پذیر نمی باشد

آیا با مشکل عدم اعتماد به گواهینامه یک منزلگاه اینترنتی مواجه شده اید؟



امنیت داده در رایانش ابری

رمز گذاری جستجوپذیر متقارن

رمز گذاری جستجوپذیر نامتقارن

رمز گذاری تمام هم ریخت

برون سپاری امن پایگاه داده و

رویکردهای تامین محرمانگی

وارسی صحت پاسخ پرسمان روی

پایگاه داده برون سپاری شده

روشهای ذخیره سازی داده های

رمز شده غیر تکراری در ابر

مروری بر محصولات موجود

در زمینه برون سپاری امن داده

امنیت داده و مدیریت مخاطرات

در رایانش ابری

آیا تا کنون نگران حریم خصوصی خود در زمان ارائه اطلاعات بوده اید؟

نام پدر :

شماره شناسنامه :

جنسیت : یکی را انتخاب کنید

تاریخ تولد : سال / ماه / روز

شغل : نام مشخص

تحصیلات : نام مشخص

شماره تلفن همراه :

تلفن :

کشور : ایران

استان : نام مشخص

شهر محل سکونت :

کد پستی :

آدرس پستی :

ارسال عکس : Browse

ارسال تصویر شناسنامه : Browse

بازگشت ثبت اطلاعات

عضویت اولیه

نام :

نام خانوادگی :

کد ملی :

آدرس پست الکترونیک :

شماره تلفن همراه :

ادامه ثبت اطلاعات بازگشت

ارسال عکس : Browse

ارسال تصویر شناسنامه : Browse

امنیت داده در رایانش ابری

رمز گذاری جستجوپذیر متقارن

رمز گذاری جستجوپذیر نامتقارن

رمز گذاری تمام هم ریخت

برون سپاری امن پایگاه داده و

رویکردهای تامین محرمانگی

وارسی صحت پاسخ پرسمان روی

پایگاه داده برون سپاری شده

روشهای ذخیره سازی داده های

رمز شده غیر تکراری در ابر

مروری بر محصولات موجود

در زمینه برون سپاری امن داده

امنیت داده و مدیریت مخاطرات

در رایانش ابری

امنیت داده در رایانش ابری

رمز گذاری جستجوپذیر متقارن

رمز گذاری جستجوپذیر نامتقارن

رمز گذاری تمام همریخت

برون سپاری امن پایگاه داده و
رویکردهای تامین محرمانگی

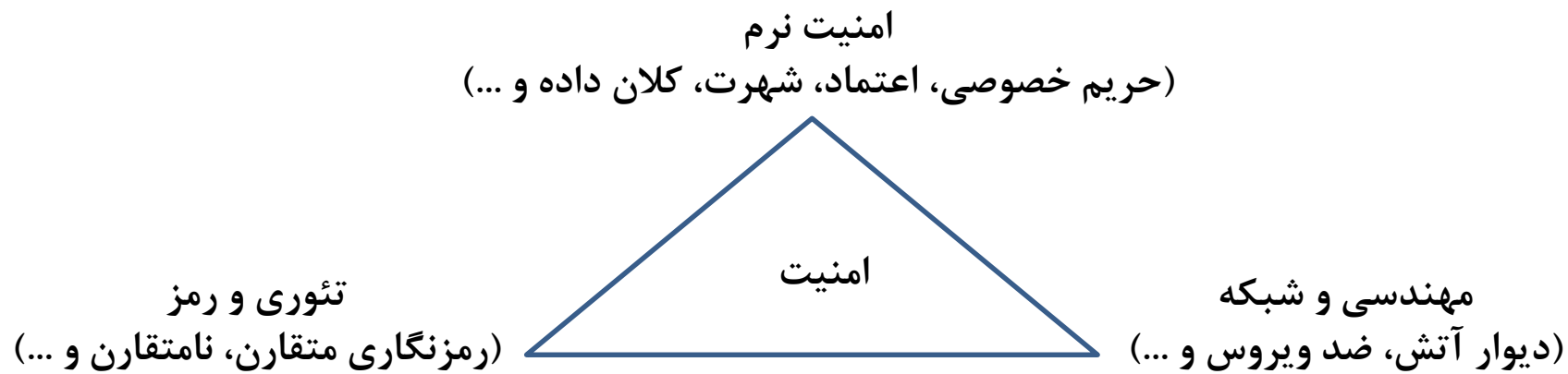
وارسی صحت پاسخ پرسمان روی
پایگاه داده برون سپاری شده

روشهای ذخیره سازی داده های
رمز شده غیر تکراری در ابر

مروری بر محصولات موجود
در زمینه برون سپاری امن داده

امنیت داده و مدیریت مخاطرات
در رایانش ابری

مدیریت مخاطرات



ابعاد مخاطرات امنیتی (مثال)

امنیت داده در رایانش ابری

رمز گذاری جستجوپذیر متقارن

رمز گذاری جستجوپذیر نامتقارن

رمز گذاری تمام هم ریخت

برون سپاری امن پایگاه داده و

رویکردهای تامین محرمانگی

وارسی صحت پاسخ پرسمان روی

پایگاه داده برون سپاری شده

روشهای ذخیره سازی داده های

رمز شده غیر تکراری در ابر

مروری بر محصولات موجود

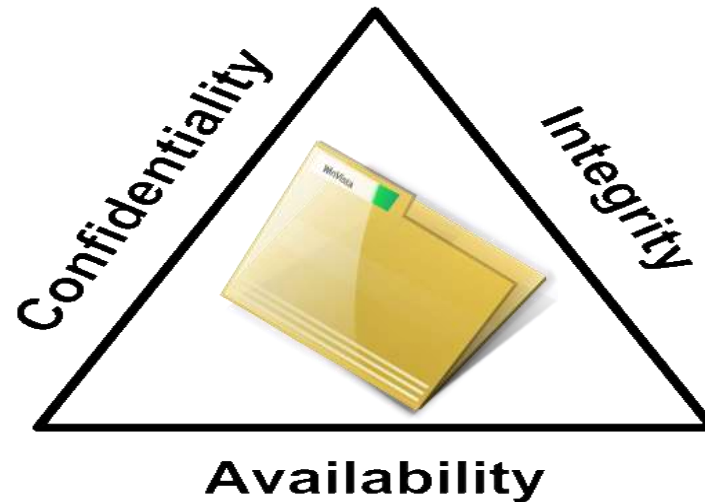
در زمینه برون سپاری امن داده

امنیت داده و مدیریت مخاطرات

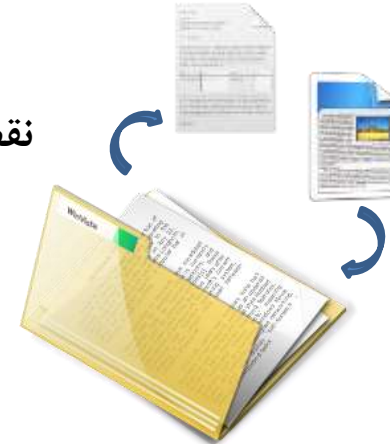
در رایانش ابری



نقض محرمانگی داده



نقض صحت داده



از دسترس خارج شدن داده



نمایش



امنیت داده در رایانش ابری

رمز گذاری جستجوپذیر متقارن

رمز گذاری جستجوپذیر نامتقارن

رمز گذاری تمام هم ریخت

برون سپاری امن پایگاه داده و

رویکردهای تامین محرمانگی

وارسی صحت پاسخ پرسمان روی

پایگاه داده برون سپاری شده

روشهای ذخیره سازی داده های

رمز شده غیر تکراری در ابر

مروری بر محصولات موجود

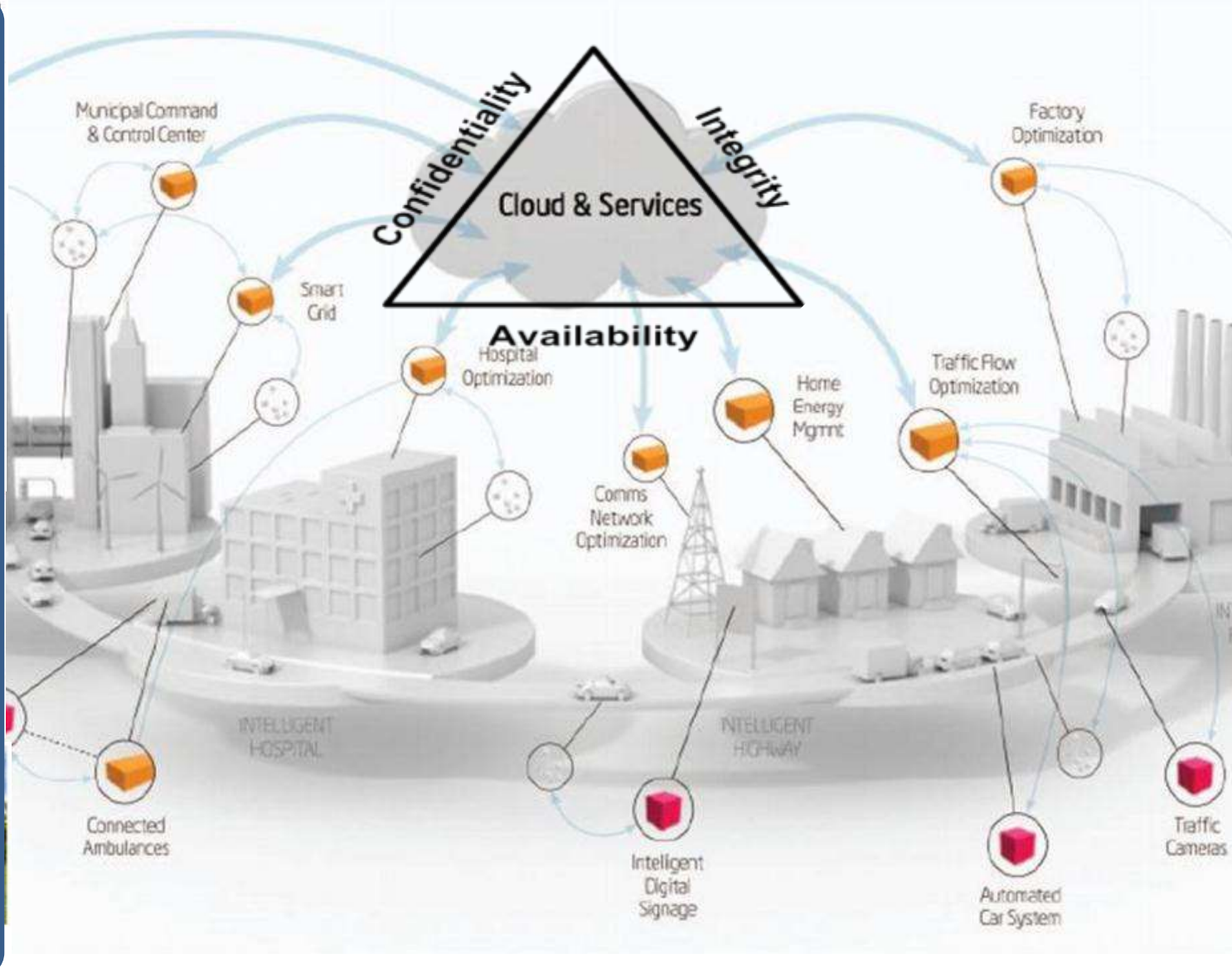
در زمینه برون سپاری امن داده

امنیت داده و مدیریت مخاطرات

در رایانش ابری

رایانش ابری: صنعت همگانی پنجم ...

- Business / Process
- Application
- Data
- Runtime / API
- Middleware
- OS
- Virtualization
- Hypervisor
- Server
- Storage
- Networking



Smart Oil



Smart logistics



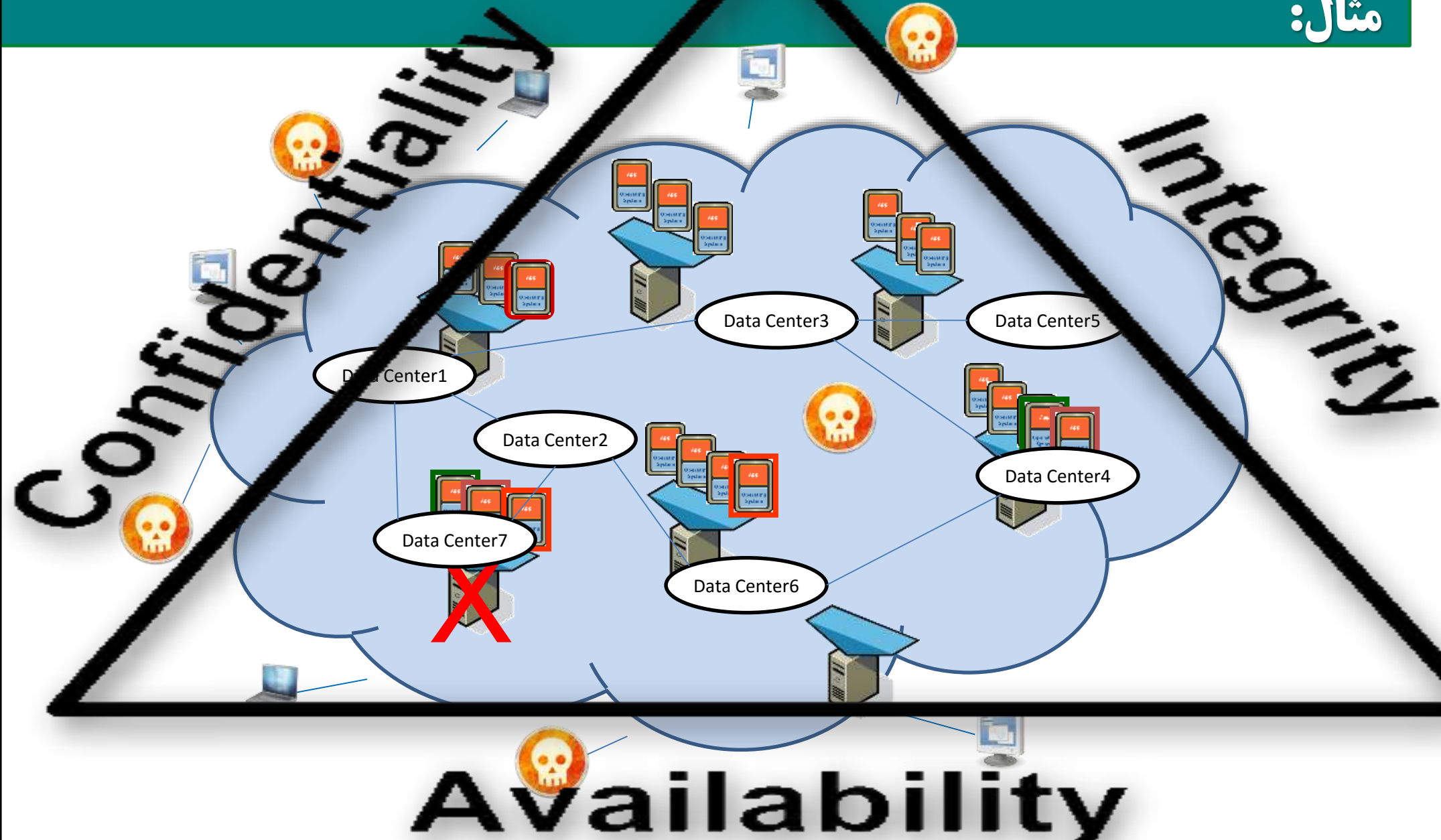
Smart consumer products



Smart banking

- امنیت داده در رایانش ابری
- رمز گذاری جستجوپذیر متقارن
- رمز گذاری جستجوپذیر نامتقارن
- رمز گذاری تمام هم ریخت
- برون سپاری امن پایگاه داده و رویکردهای تامین محرمانگی
- وارسی صحت پاسخ پرسمان روی پایگاه داده برون سپاری شده
- روشهای ذخیره سازی داده های رمز شده غیر تکراری در ابر
- مروری بر محصولات موجود در زمینه برون سپاری امن داده
- امنیت داده و مدیریت مخاطرات در رایانش ابری

مثال:



- امنیت داده در رایانش ابری
- رمز گذاری جستجوپذیر متقارن
- رمز گذاری جستجوپذیر نامتقارن
- رمز گذاری تمام هم ریخت
- برون سپاری امن پایگاه داده و رویکردهای تامین محرمانگی
- وارسی صحت پاسخ پرسمان روی پایگاه داده برون سپاری شده
- روشهای ذخیره سازی داده های رمز شده غیر تکراری در ابر
- مروری بر محصولات موجود در زمینه برون سپاری امن داده
- امنیت داده و مدیریت مخاطرات در رایانش ابری

مثال: (نقض صحت)

Memory Viewer

File Search View Debug Tools Kernel tools

Tutorial-i386.exe+2552F

Address	Bytes	Opcode	Con
Tutorial-i386.85 C0		test eax, eax	
Tutorial-i386.0F85 C3000000		jne Tutorial-i386.exe+255FA	
Tutorial-i386.8B B3 78040000		mov esi, [ebx+00000478]	
Tutorial-i386.83 AB 78040000 01		sub dword ptr [ebx+00000478], 01	1
Tutorial-i386.8B 83 78040000		mov eax, [ebx+00000478]	
Tutorial-i386.8D 55 D4		lea edx, [ebp-2C]	
Tutorial-i386.E8 BE470100		call Tutorial-i386.exe+39D10	
Tutorial-i386.8B 55 D4		mov edx, [ebp-2C]	
Tutorial-i386.8B 83 6C040000		mov eax, [ebx+0000046C]	
Tutorial-i386.E8 E0E00600		call Tutorial-i386.exe+93640	
Tutorial-i386.8B 93 78040000		mov edx, [ebx+00000478]	
Tutorial-i386.89 D0		mov eax, edx	

subtract

Protect:Execute/Read only Base=72922000 Size=69000 Module=apphelp.dll

address	1E	1F	20	21	22	23	24	25	EF012345
7292271E	FF	75	0C	FF	15	14	F2	98	u..
72922726	72	59	59	85	C0	74	97	46	rYY t F
7292272E	83	C7	10	83	FE	0F	72	E6	. .r
72922736	8B	4D	FC	8B	C3	5F	5E	33	M . ^3
7292273E	CD	5B	E8	2B	F2	FE	FF	8B	[+
72922746	E5	5D	C2	0C	00	6A	01	50] ..j.P
7292274E	FF	B5	E0	FD	FF	FF	E8	17	.
72922756	00	00	00	89	85	C8	FD	FF	...
7292275E	FF	E9	37	88	FF	FF	90	90	7
72922766	90	90	90	90	90	90	90	90	
7292276E	90	90	90	90	90	90	90	90	
72922776	EC	0C	83	65	F8	00	8D	45	. e . E
7292277E	FC	83	65	FC	00	50	8D	45	e .P E
72922786	F8	50	FF	75	0C	FF	75	08	P u . u .
7292278E	E8	AD	41	FF	FF	85	C0	0F	A . .
72922796	84	52	23	02	00	FF	75	10	R#.. u .
7292279E	FF	75	FC	FF	75	F8	E8	27	u u '
729227A6	44	FF	FF	8B	E5	5D	C2	0C	D] .
729227AE	00	90	55	53	45	52	33	32	. USER32
729227B6	2E	44	4C	4C	00	8B	8D	70	.DLL. p

Address	Bytes	Opcode	Con
Tutorial-i386.85 C0		test eax, eax	
Tutorial-i386.0F85 C3000000		jne Tutorial-i386.exe+255FA	
Tutorial-i386.8B B3 78040000		mov esi, [ebx+00000478]	
Tutorial-i386.83 AB 78040000 01		sub dword ptr [ebx+00000478], 01	1
Tutorial-i386.8B 83 78040000		mov eax, [ebx+00000478]	
Tutorial-i386.8D 55 D4		lea edx, [ebp-2C]	
Tutorial-i386.E8 BE470100		call Tutorial-i386.exe+39D10	

Address	Bytes	Opcode	Con
Tutorial-i386.85 C0		test eax, eax	
Tutorial-i386.0F85 C3000000		jne Tutorial-i386.exe+255FA	
Tutorial-i386.8B B3 78040000		mov esi, [ebx+00000478]	
Tutorial-i386.E9 BEAA3901		jmp 017C0000	
Tutorial-i386.90		nop	
Tutorial-i386.90		nop	
Tutorial-i386.8B 83 78040000		mov eax, [ebx+00000478]	
Tutorial-i386.8D 55 D4		lea edx, [ebp-2C]	

Address	Bytes	Opcode	Con
017C0000	83 83 78040000 02	add dword ptr [ebx+00000478], 02	2
017C0007	E9 3855C6FE	jmp Tutorial-i386.exe+25544	

امنیت داده در رایانش ابری

رمز گذاری جستجوپذیر متقارن

رمز گذاری جستجوپذیر نامتقارن

رمز گذاری تمام هم ریخت

برون سپاری امن پایگاه داده و

رویکردهای تامین محرمانگی

وارسی صحت پاسخ پرسمان روی

پایگاه داده برون سپاری شده

روشهای ذخیره سازی داده های

رمز شده غیر تکراری در ابر

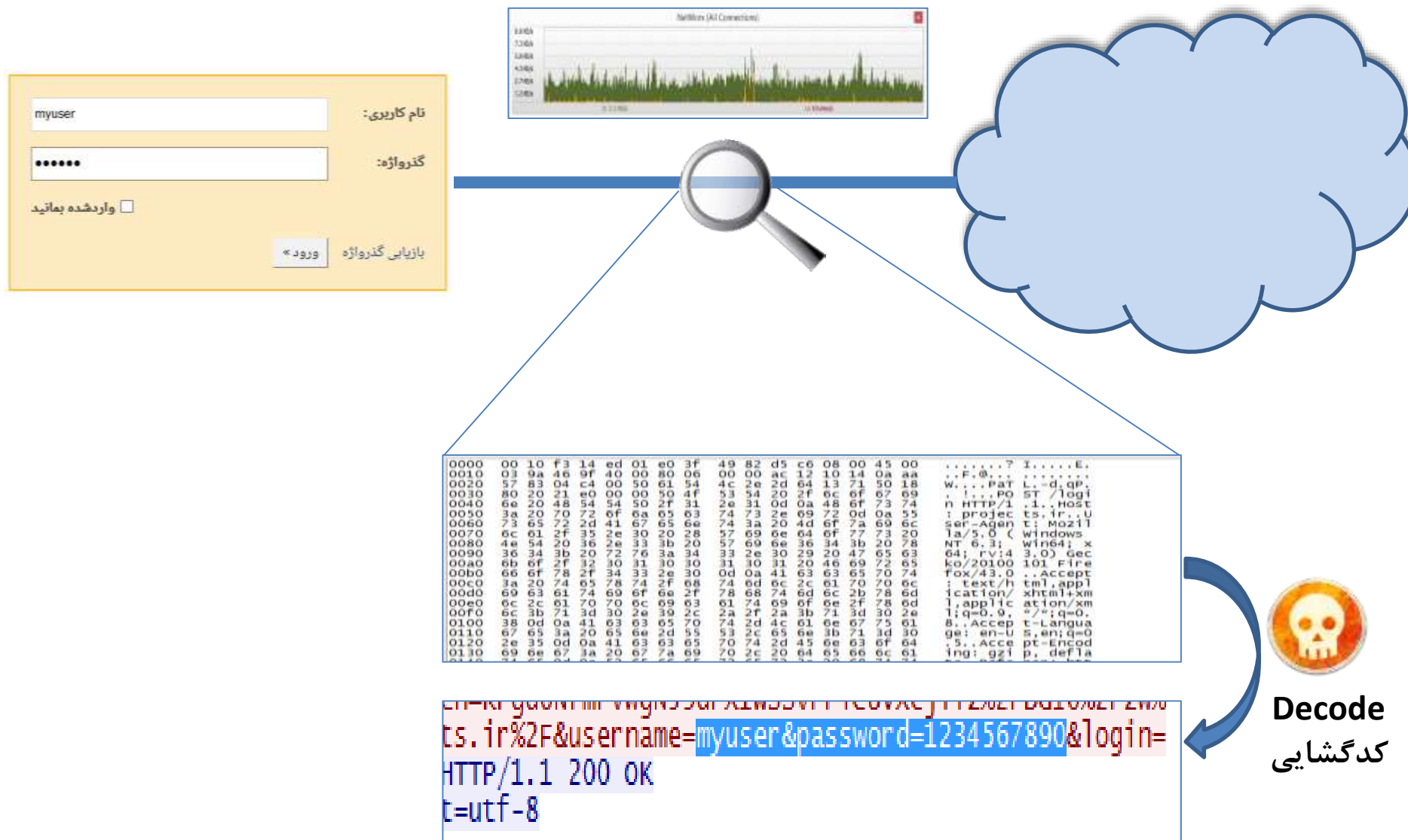
مروری بر محصولات موجود

در زمینه برون سپاری امن داده

امنیت داده و مدیریت مخاطرات

در رایانش ابری

مثال: (نقض محرمانگی)



امنیت داده در رایانش ابری

رمز گذاری جستجوپذیر متقارن

رمز گذاری جستجوپذیر نامتقارن

رمز گذاری تمام هم ریخت

برون سپاری امن پایگاه داده و

رویکردهای تامین محرمانگی

وارسی صحت پاسخ پرسمان روی

پایگاه داده برون سپاری شده

روشهای ذخیره سازی داده های

رمز شده غیر تکراری در ابر

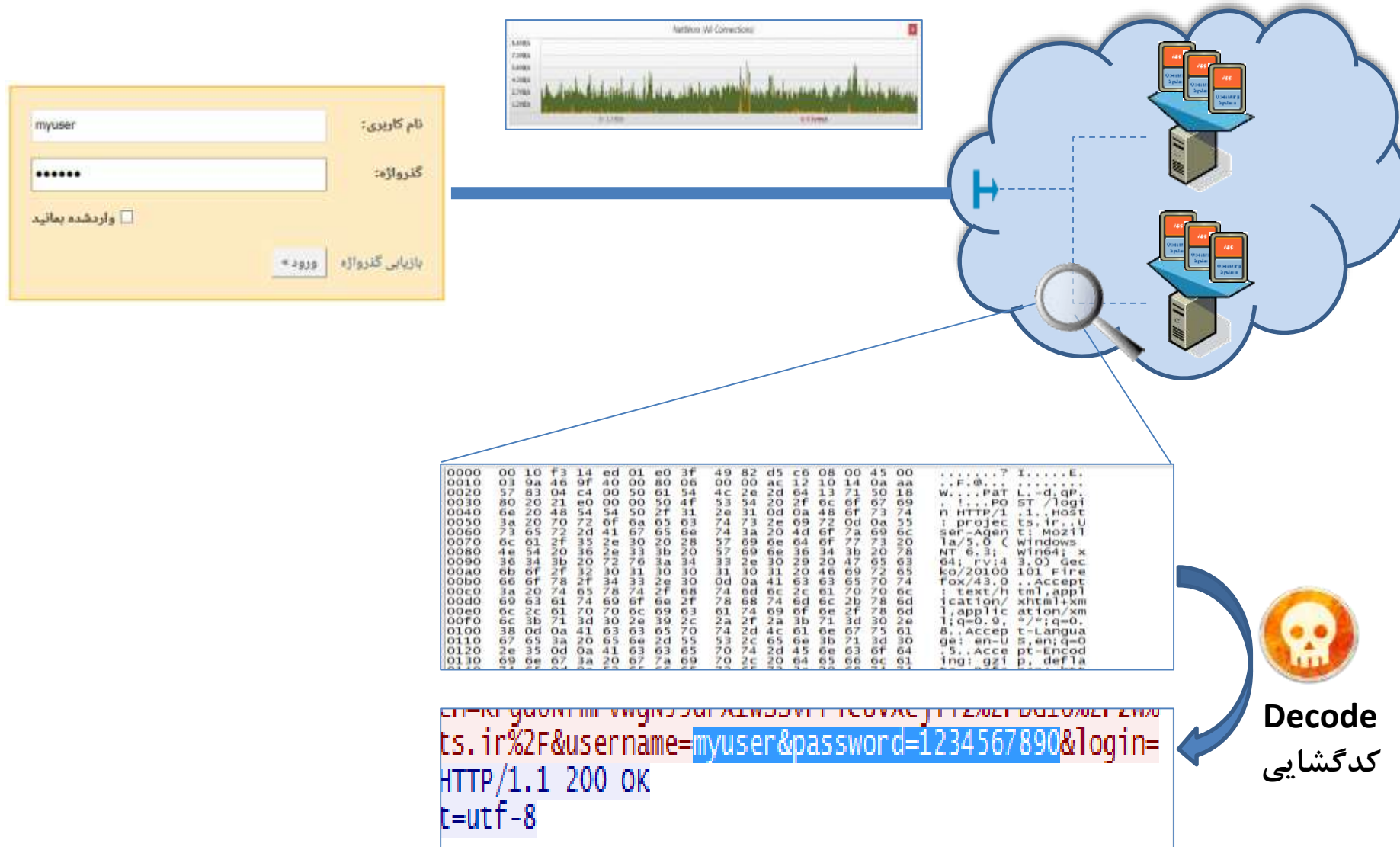
مروری بر محصولات موجود

در زمینه برون سپاری امن داده

امنیت داده و مدیریت مخاطرات

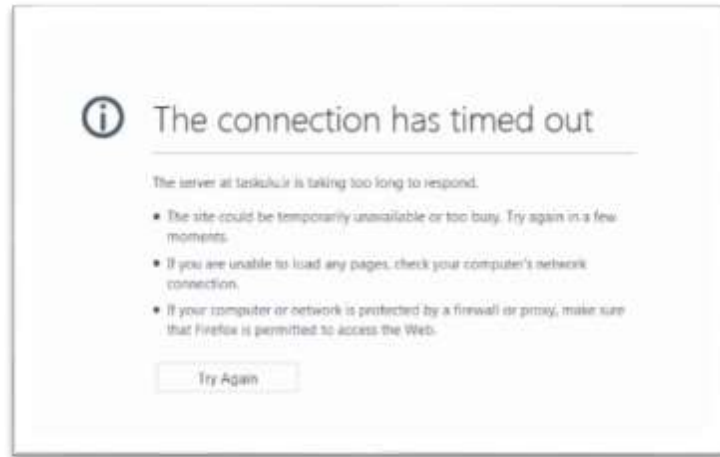
در رایانش ابری

مثال: (نقض محرمانگی)



- امنیت داده در رایانش ابری
- رمز گذاری جستجوپذیر متقارن
- رمز گذاری جستجوپذیر نامتقارن
- رمز گذاری تمام هم ریخت
- برون سپاری امن پایگاه داده و رویکردهای تامین محرمانگی
- وارسی صحت پاسخ پرسمان روی پایگاه داده برون سپاری شده
- روشهای ذخیره سازی داده های رمز شده غیر تکراری در ابر
- مروری بر محصولات موجود در زمینه برون سپاری امن داده
- امنیت داده و مدیریت مخاطرات در رایانش ابری

مثال: (نقض دسترسی)



امنیت داده در رایانش ابری

رمز گذاری جستجوپذیر متقارن

رمز گذاری جستجوپذیر نامتقارن

رمز گذاری تمام هم ریخت

برون سپاری امن پایگاه داده و

رویکردهای تامین محرمانگی

وارسی صحت پاسخ پرسمان روی

پایگاه داده برون سپاری شده

روشهای ذخیره سازی داده های

رمز شده غیر تکراری در ابر

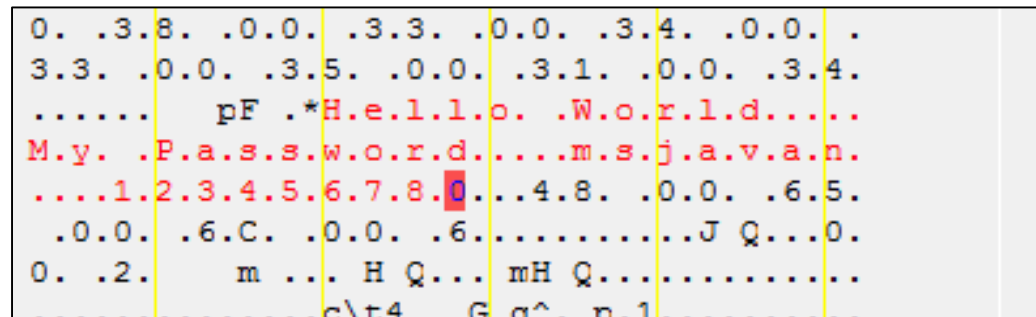
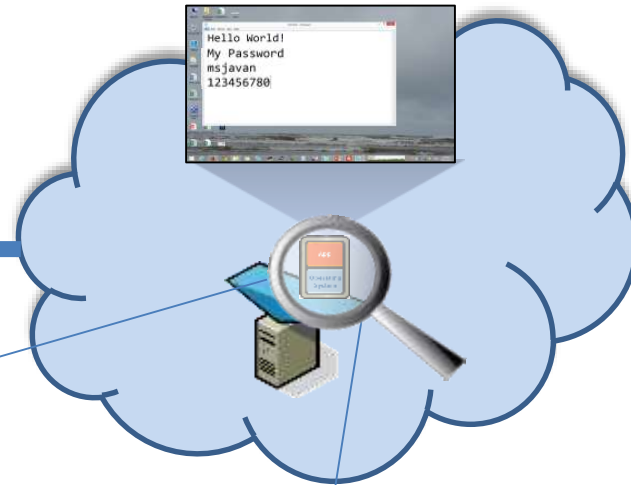
مروری بر محصولات موجود

در زمینه برون سپاری امن داده

امنیت داده و مدیریت مخاطرات

در رایانش ابری

مثال: (نقض محرمانگی و صحت)



Decode
کدگشایی

امنیت داده در رایانش ابری

رمز گذاری جستجوپذیر متقارن

رمز گذاری جستجوپذیر نامتقارن

رمز گذاری تمام هم ریخت

برون سپاری امن پایگاه داده و

رویکردهای تامین محرمانگی

وارسی صحت پاسخ پرسمان روی

پایگاه داده برون سپاری شده

روشهای ذخیره سازی داده های

رمز شده غیر تکراری در ابر

مروری بر محصولات موجود

در زمینه برون سپاری امن داده

امنیت داده و مدیریت مخاطرات

در رایانش ابری

مثال موردی: VDI

امنیت داده در رایانش ابری

رمز گذاری جستجوپذیر متقارن

رمز گذاری جستجوپذیر نامتقارن

رمز گذاری تمام هم ریخت

برون سپاری امن پایگاه داده و

رویکردهای تامین محرمانگی

وارسی صحت پاسخ پرسمان روی

پایگاه داده برون سپاری شده

روشهای ذخیره سازی داده های

رمز شده غیر تکراری در ابر

مروری بر محصولات موجود

در زمینه برون سپاری امن داده

امنیت داده و مدیریت مخاطرات

در رایانش ابری

```

1 [|||||]
2 [|||||]
3 [|||||]
4 [|||||]
Mem [|||||]
Swp [|||||]

```

PID	USER	PRI	NI	VRT	RES	SHR	S	CPU%	MEM%	T
3058	libvirt-q	20	0	4546M	2952M	2088	S	15.8	9.2	2h
4795	libvirt-q	20	0	4546M	2972M	2112	S	11.2	9.2	2h
4982	libvirt-q	20	0	4546M	2972M	2100	R	11.2	9.2	2h
3829	libvirt-q	20	0	4547M	549M	2096	S	10.5	1.7	2h
4854	libvirt-q	20	0	4546M	2988M	2088	S	9.8	9.3	2h
5579	libvirt-q	20	0	4546M	2969M	2392	S	9.8	9.2	2h
3523	libvirt-q	20	0	4546M	2950M	2092	R	9.8	9.2	2h
2969	libvirt-q	20	0	4546M	2882M	2076	R	9.2	9.0	2h
3106	libvirt-q	20	0	4546M	2908M	2076	S	9.2	9.0	2h
1306	root	20	0	1008M	15592	4496	S	7.2	0.0	7:
3059	libvirt-q	20	0	4546M	2952M	2088	S	4.6	9.2	15:
26905	morteza	20	0	586M	61708	17180	S	3.9	0.2	0:
3060	libvirt-q	20	0	4546M	2952M	2088	S	3.3	9.2	8:
4798	libvirt-q	20	0	4546M	2972M	2112	S	1.3	9.2	15:
27317	morteza	20	0	26600	2752	1448	R	1.3	0.0	0:
5580	libvirt-q	20	0	4546M	2969M	2392	S	1.3	9.2	15:
3107	libvirt-q	20	0	4546M	2908M	2076	S	1.3	9.0	15:
4855	libvirt-q	20	0	4546M	2988M	2088	S	1.3	9.3	15:
3524	libvirt-q	20	0	4546M	2950M	2092	S	1.3	9.2	15:
2970	libvirt-q	20	0	4546M	2882M	2076	S	1.3	9.0	15:
5637	libvirt-q	20	0	4548M	178M	2360	S	1.3	0.6	8:
3108	libvirt-q	20	0	4546M	2908M	2076	S	1.3	9.0	9:
1310	root	20	0	1008M	15592	4496	S	1.3	0.0	0:
5498	libvirt-q	20	0	4546M	2917M	2356	S	1.3	9.1	8:
5581	libvirt-q	20	0	4546M	2969M	2392	S	1.3	9.2	8:
26756	morteza	20	0	123M	2644	1360	S	0.7	0.0	0:
4799	libvirt-q	20	0	4546M	2972M	2112	S	0.7	9.2	8:
3833	libvirt-q	20	0	4547M	549M	2096	S	0.7	1.7	14:
4983	libvirt-q	20	0	4546M	2972M	2100	S	0.7	9.2	15:
1309	root	20	0	1008M	15592	4496	S	0.7	0.0	0:
3834	libvirt-q	20	0	4547M	549M	2096	S	0.7	1.7	8:
4984	libvirt-q	20	0	4546M	2972M	2100	S	0.7	9.2	8:

Virtual Machine Manager@zdesk1

File Edit View Help

New Open Run Pause Shutdown

Name	CPU usage	Host CPU usage	Disk I/O	Network I/O
192.168.1.211 (QEMU) - Not Connected				
localhost (QEMU)				
xp				
Running				
xp-user0				
Running				
xp-user1				
Running				
xp-user10				
Paused				
xp-user11				
Running				
xp-user2				
Shutoff				
xp-user3				
Running				
xp-user4				
Running				
xp-user5				
Paused				
xp-user6				
Running				
xp-user7				

F1 Help F2 Setup F3 Search F4 Filter F5 Tree F6 SortBy F7 Nice F8

مثال موردی: VDI

امنیت داده در رایانش ابری

رمز گذاری جستجوپذیر متقارن

رمز گذاری جستجوپذیر نامتقارن

رمز گذاری تمام هم ریخت

برون سپاری امن پایگاه داده و

رویکردهای تامین محرمانگی

وارسی صحت پاسخ پرسمان روی

پایگاه داده برون سپاری شده

روشهای ذخیره سازی داده های

رمز شده غیر تکراری در ابر

مروری بر محصولات موجود

در زمینه برون سپاری امن داده

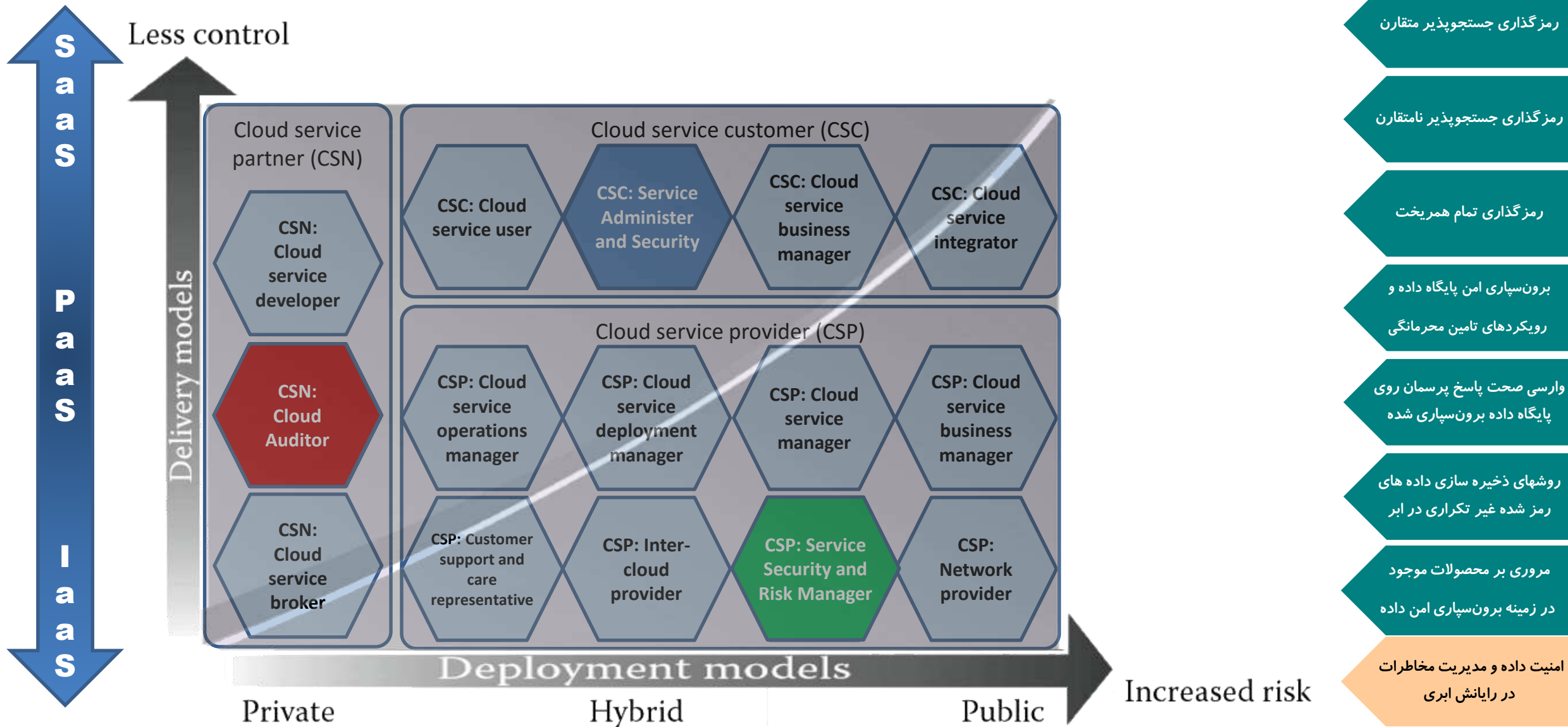
امنیت داده و مدیریت مخاطرات

در رایانش ابری

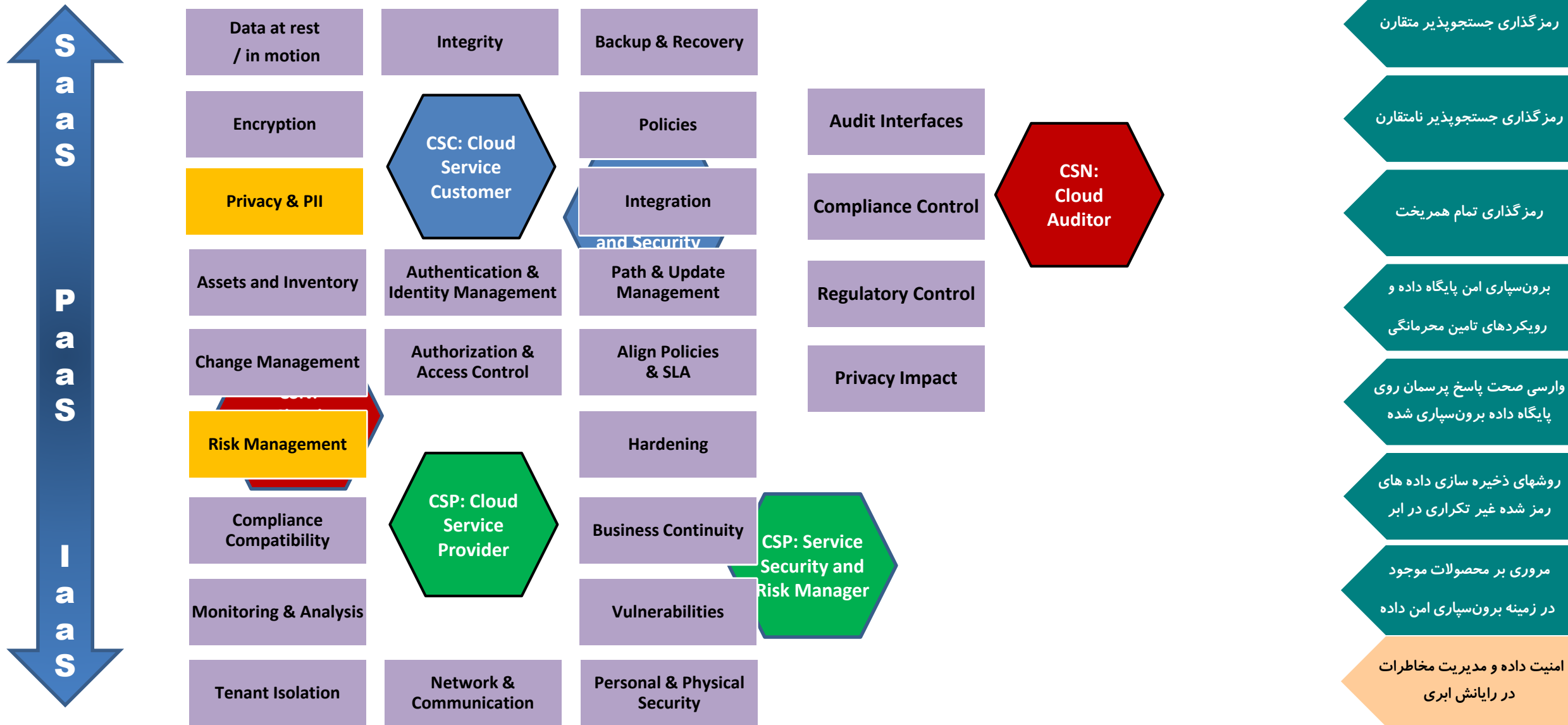
The image displays a terminal window with system statistics and a list of processes. The statistics include CPU usage (14.6% to 17.6%), memory usage (3415/32174MB), and tasks (97, 182 thr; 2 running). The process list shows various users (root, libvirt-q, morteza) and their CPU/MEM usage. Below the terminal is a screenshot of the Virtual Machine Manager interface, showing a list of VMs with columns for Name, CPU usage, Host CPU usage, Disk I/O, and Network I/O. The VMs listed include 'xp', 'xp-user0', 'xp-user1', and 'xp-user10'.

PID	USER	PRI	NI	VIRT	RES	SHR	S	CPU%	MEM%	TIME+	Command
1306	root	20	0	1008M	15592	4496	S	14.5	0.0	7:42.01	/usr/sbin/libvirtd -d -l
4854	libvirt-q	20	0	4546M	2988M	2088	S	10.6	9.3	2h23:48	qemu-system-x86_64 -enable-kvm -name xp-user3 -S -machine pc-i440fx-trusty,accel=kvm,usb=off -m 4024 -
4982	libvirt-q	20	0	4546M	2972M	2100	S	9.9	9.2	2h23:37	qemu-system-x86_64 -enable-kvm -name xp-user8 -S -machine pc-i440fx-trusty,accel=kvm,usb=off -m 4024 -
3829	libvirt-q	20	0	4547M	549M	2096	R	9.9	1.7	2h24:04	qemu-system-x86_64 -enable-kvm -name xp-user11 -S -machine pc-i440fx-trusty,accel=kvm,usb=off -m 4024 -
3106	libvirt-q	20	0	4546M	2908M	2076	S	9.9	9.0	2h24:55	qemu-system-x86_64 -enable-kvm -name xp-user6 -S -machine pc-i440fx-trusty,accel=kvm,usb=off -m 4024 -
3523	libvirt-q	20	0	4546M	2950M	2092	S	9.9	9.2	2h24:48	qemu-system-x86_64 -enable-kvm -name xp-user1 -S -machine pc-i440fx-trusty,accel=kvm,usb=off -m 4024 -
2969	libvirt-q	20	0	4546M	2882M	2076	S	9.9	9.0	2h24:09	qemu-system-x86_64 -enable-kvm -name xp-user0 -S -machine pc-i440fx-trusty,accel=kvm,usb=off -m 4024 -
3058	libvirt-q	20	0	4546M	2952M	2088	S	9.9	9.2	2h25:26	qemu-system-x86_64 -enable-kvm -name xp-user4 -S -machine pc-i440fx-trusty,accel=kvm,usb=off -m 4024 -
5579	libvirt-q	20	0	4546M	2969M	2392	S	9.9	9.2	2h	
4795	libvirt-q	20	0	4546M	2972M	2112	S	9.2	9.2	2h	
6905	morteza	20	0	586M	61708	17180	S	6.6	0.2	0:0	
7317	morteza	20	0	26600	2752	1448	R	1.3	0.0	0:0	
4855	libvirt-q	20	0	4546M	2988M	2088	S	1.3	9.3	15:	
4983	libvirt-q	20	0	4546M	2972M	2100	S	1.3	9.2	15:	
4798	libvirt-q	20	0	4546M	2972M	2112	S	1.3	9.2	15:	
3833	libvirt-q	20	0	4547M	549M	2096	S	1.3	1.7	14:	
3107	libvirt-q	20	0	4546M	2908M	2076	S	1.3	9.0	15:	
3524	libvirt-q	20	0	4546M	2950M	2092	S	1.3	9.2	15:	
1310	root	20	0	1008M	15592	4496	S	1.3	0.0	0:0	
1318	root	20	0	1008M	15592	4496	S	1.3	0.0	0:0	
5580	libvirt-q	20	0	4546M	2969M	2392	S	0.7	9.2	15:	
2970	libvirt-q	20	0	4546M	2882M	2076	S	0.7	9.0	15:	
3059	libvirt-q	20	0	4546M	2952M	2088	S	0.7	9.2	15:	
5637	libvirt-q	20	0	4548M	178M	2360	S	0.7	0.6	8:	
1313	root	20	0	1008M	15592	4496	S	0.7	0.0	0:0	
1309	root	20	0	1008M	15592	4496	S	0.7	0.0	0:0	
1311	root	20	0	1008M	15592	4496	S	0.7	0.0	0:0	
3525	libvirt-q	20	0	4546M	2950M	2092	S	0.7	9.2	8:	
2971	libvirt-q	20	0	4546M	2882M	2076	S	0.7	9.0	8:	
1312	root	20	0	1008M	15592	4496	S	0.7	0.0	0:0	
1314	root	20	0	1008M	15592	4496	S	0.7	0.0	0:0	
4984	libvirt-q	20	0	4546M	2972M	2100	S	0.7	9.2	8:	

معماری مرجع رایانش ابری: ISO/IEC 17789: 2014



نقش های امنیتی در معماری مرجع رایانش ابری: ISO/IEC 17789: 2014



مدیریت مخاطرات (گزارش نسخه ۲۰۱۲)

قفل شدن در فروشنده
(Vendor Lock-in)

احضاریه
(Subpoena)

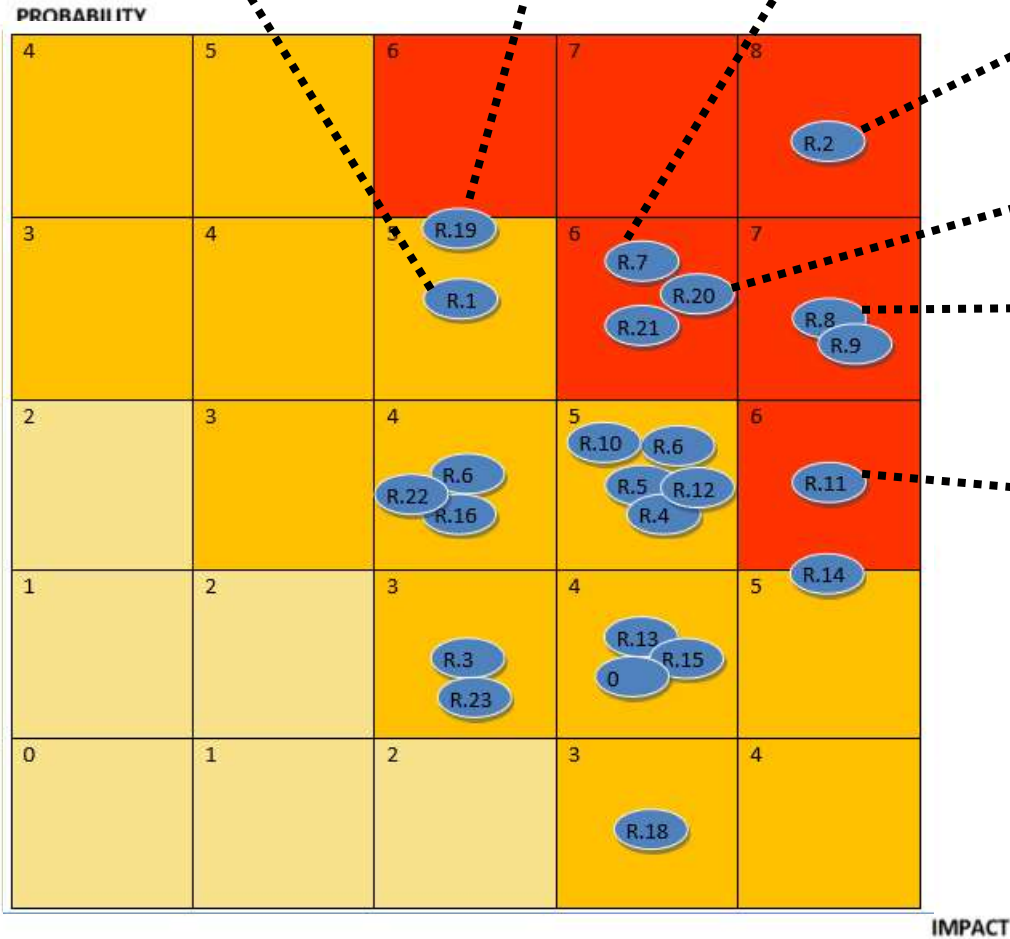
شکست جداسازی
(Isolation Failure)

از دست دادن کنترل
(Loss of Governance)

خطر تغییر حوزه قضایی
(Change of jurisdiction)

کاربر داخلی بدخواه
(Malicious Insider)

حذف داده به صورت غیر امن
(Insecure deletion of data)



- تحلیل دارایی ها
- تحلیل مخاطرات
- ارایه راهکار

امنیت داده در رایانش ابری

رمز گذاری جستجوپذیر متقارن

رمز گذاری جستجوپذیر نامتقارن

رمز گذاری تمام هم ریخت

برون سپاری امن پایگاه داده و

رویکردهای تامین محرمانگی

وارسی صحت پاسخ پرسمان روی

پایگاه داده برون سپاری شده

روشهای ذخیره سازی داده های

رمز شده غیر تکراری در ابر

مروری بر محصولات موجود

در زمینه برون سپاری امن داده

امنیت داده و مدیریت مخاطرات

در رایانش ابری

□ تحلیل موردی مخاطرات خدمت پیغام رسانی

- قفل شدن در فروشنده (Vendor Lock-in)
- از دست دادن کنترل (Loss of Governance)
- شکست زنجیره تامین (Supply chain failure)
- شکست جداسازی (Isolation Failure)
- کاربر داخلی بدخواه (Malicious Insider)
- حمله منع خدمت (Denial of Service)
- حذف داده به صورت غیر امن (Insecure deletion of data)
- از دست دادن کلیدهای رمزنگاشتی (Loss of Cryptographic Keys)



مخاطره قفل شدن در فروشنده (Lock-in)

امنیت داده در رایانش ابری

رمز گذاری جستجوپذیر متقارن

رمز گذاری جستجوپذیر نامتقارن

رمز گذاری 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 مخاطرات

در رایانش ابری

□ زمانی که خدمت قابل جابجایی نباشد و یا امکان مهاجرت از یک کارگزار به دیگری وجود نداشته باشد.



□ مثالی از مواردی که ریسک Lock-in پایین است:
○ جابجایی خدمت در خدمات میزبانی / ترابرد بین اپراتورها

□ مثالی از مواردی که ریسک Lock-in بالا است:
○ نرم افزارهای پیغام رسان / خدمت پست الکترونیکی / خدمت های سفارشی مدیریت محتوا

۱

۲

۳

۴

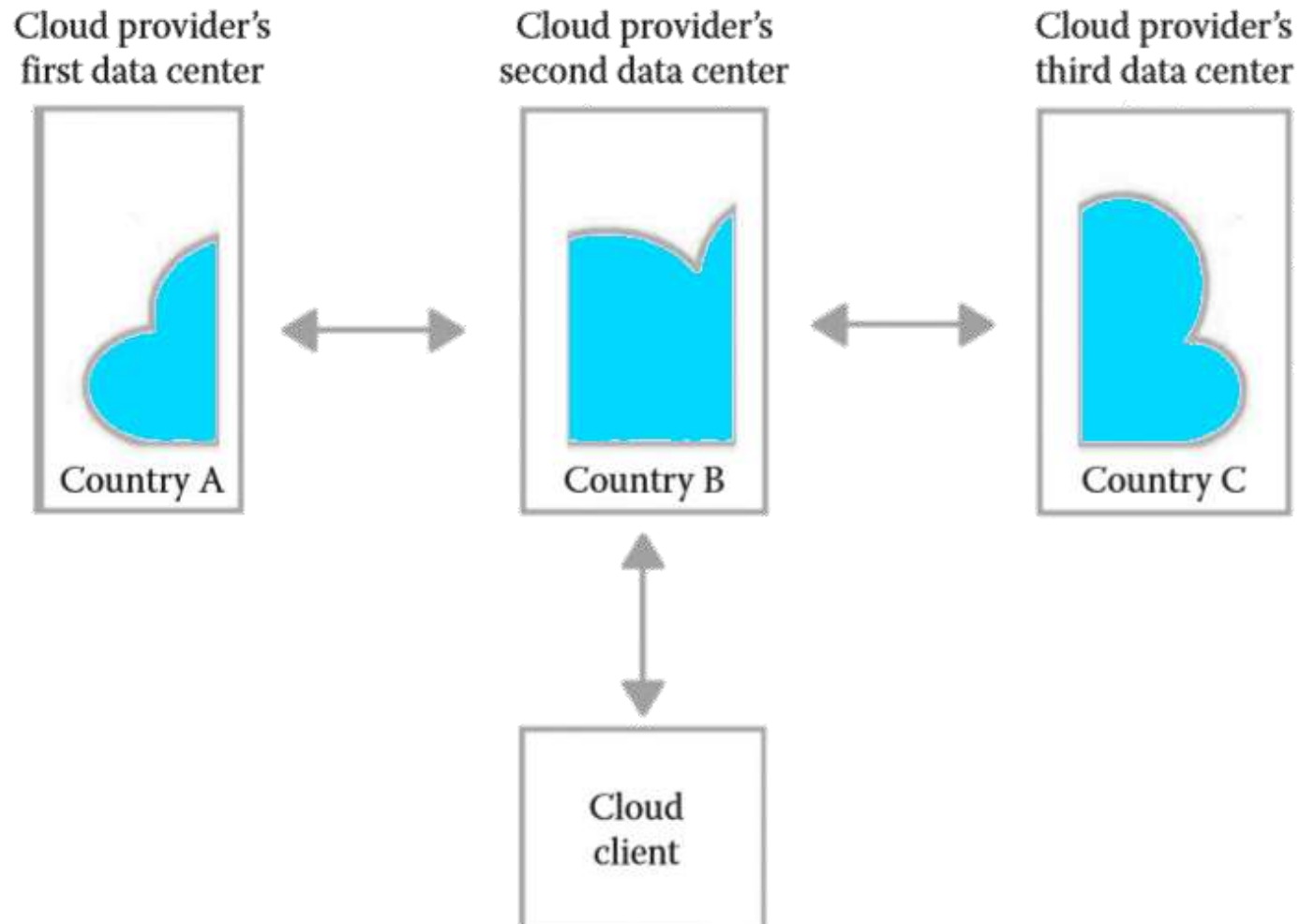
۵

۶

۷

۸

مخاطره از دست دادن کنترل (Loss of Governance)



امنیت داده در رایانش ابری

رمز گذاری جستجوپذیر متقارن

رمز گذاری جستجوپذیر نامتقارن

رمز گذاری تمام هم ریخت

برون سپاری امن پایگاه داده و

رویکردهای تامین محرمانگی

وارسی صحت پاسخ پرسمان روی

پایگاه داده برون سپاری شده

روشهای ذخیره سازی داده های

رمز شده غیر تکراری در ابر

مروری بر محصولات موجود

در زمینه برون سپاری امن داده

امنیت داده و مدیریت مخاطرات

در رایانش ابری

۱

۲

۳

۴

۵

۶

۷

۸

مخاطره از دست دادن کنترل (Loss of Governance)

امنیت داده در رایانش ابری

رمز گذاری جستجوپذیر متقارن

رمز گذاری جستجوپذیر نامتقارن

رمز گذاری تمام هم ریخت

برون سپاری امن پایگاه داده و

رویکردهای تامین محرمانگی

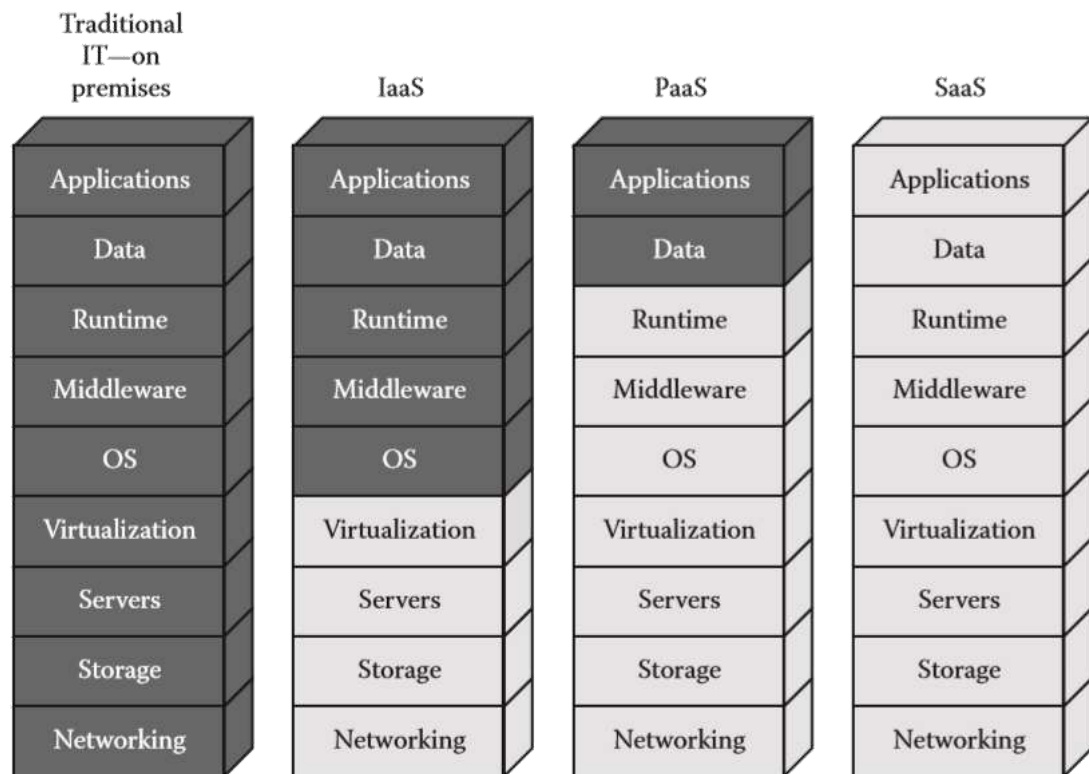
وارسی صحت پاسخ پرسمان روی
پایگاه داده برون سپاری شدهروشهای ذخیره سازی داده های
رمز شده غیر تکراری در ابر

مروری بر محصولات موجود

در زمینه برون سپاری امن داده

امنیت داده و مدیریت مخاطرات
در رایانش ابری

□ زمانی پیش می آید که امکان انجام برخی از کارها وجود نداشته باشد و یا جلوی آن گرفته شود. خصوصا در نیازمندی های امنیتی.



□ مثال:

- نداشتن کنترل بر روی محل داده
- عدم امکان بعضی از پیکربندی ها
- اختلاف نظر در Hardening
- جلوگیری از PortScan
- ...

مخاطره شکست در زنجیره تامین (Supply chain failure)

□ زمانی پیش می آید که بخشی از فرآیند یک زنجیره تامین بصورت ابری انجام شود و در صورت نقص در ارائه خدمت / نقض محرمانگی و ... ، زنجیره به خطر بیفتد.



□ مثال:

- ارسال/دریافت نیازمندی ها از طریق فکس
- جهت تایید سفارش و ارسال آن
- سفارش تاکسی / پیک بصورت ابری

امنیت داده در رایانش ابری

رمز گذاری جستجوپذیر متقارن

رمز گذاری جستجوپذیر نامتقارن

رمز گذاری تمام همریخت

برون سپاری امن پایگاه داده و

رویکردهای تامین محرمانگی

وارسی صحت پاسخ پرسمان روی

پایگاه داده برون سپاری شده

روشهای ذخیره سازی داده های

رمز شده غیر تکراری در ابر

مروری بر محصولات موجود

در زمینه برون سپاری امن داده

امنیت داده و مدیریت مخاطرات

در رایانش ابری

۱

۲

۳

۴

۵

۶

۷

۸

مخاطره شکست جداسازی (Isolation Failure)

امنیت داده در رایانش ابری

رمز گذاری جستجوپذیر متقارن

رمز گذاری جستجوپذیر نامتقارن

رمز گذاری تمام هم ریخت

برون سپاری امن پایگاه داده و

رویکردهای تامین محرمانگی

وارسی صحت پاسخ پرسمان روی

پایگاه داده برون سپاری شده

روشهای ذخیره سازی داده های

رمز شده غیر تکراری در ابر

مروری بر محصولات موجود

در زمینه برون سپاری امن داده

امنیت داده و مدیریت مخاطرات

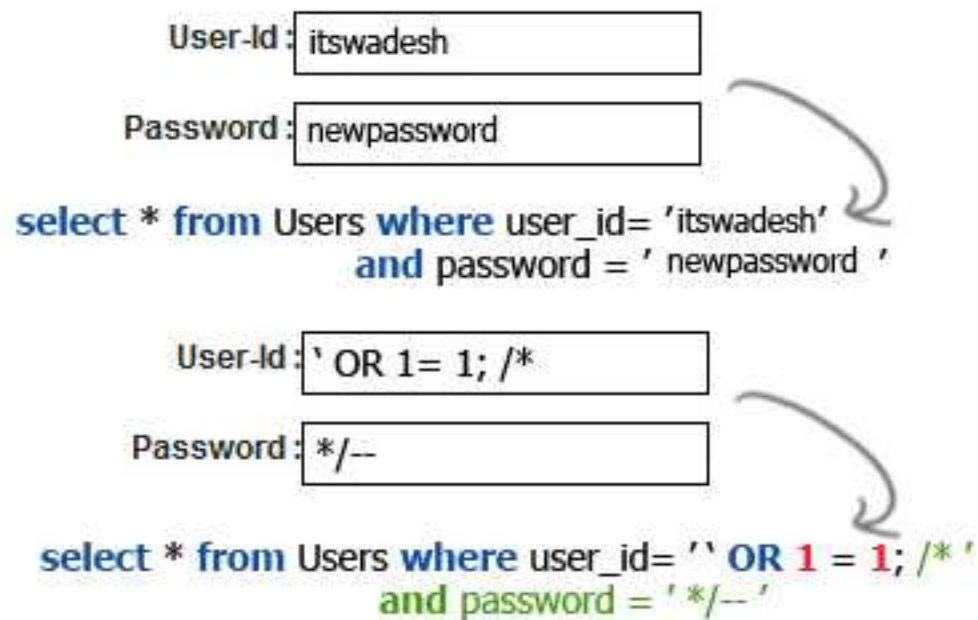
در رایانش ابری

□ مثال:

○ SQL Injection

○ Spaming

○ Filtering



۱

۲

۳

۴

۵

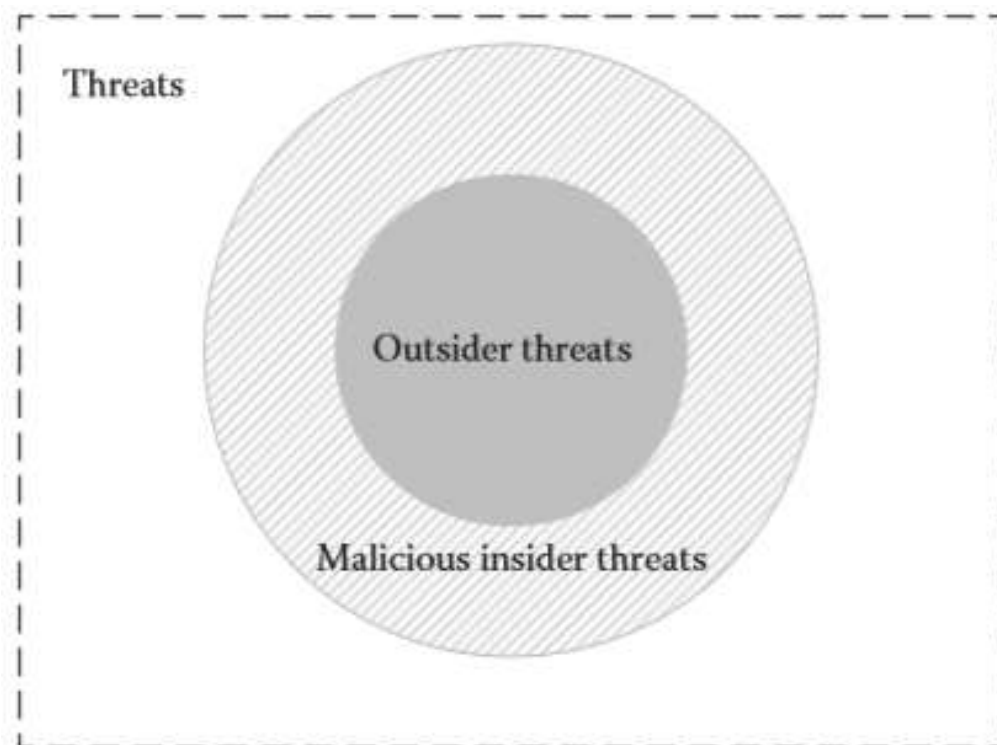
۶

۷

۸

مخاطره کاربر داخلی بدخواه (Malicious Insider)

□ زمانی اتفاق می افتد که کارمندان داخلی کارگزار ابری، از دسترسی های خود سوء استفاده کنند.



□ مثال:

- کپی اطلاعات
- تغییر اطلاعات
- حذف اطلاعات
- افشای کلمه عبور

امنیت داده در رایانش ابری

رمز گذاری جستجوپذیر متقارن

رمز گذاری جستجوپذیر نامتقارن

رمز گذاری تمام هم ریخت

برون سپاری امن پایگاه داده و

رویکردهای تامین محرمانگی

وارسی صحت پاسخ پرسمان روی

پایگاه داده برون سپاری شده

روشهای ذخیره سازی داده های

رمز شده غیر تکراری در ابر

مروری بر محصولات موجود

در زمینه برون سپاری امن داده

امنیت داده و مدیریت مخاطرات

در رایانش ابری

مخاطره حذف داده به صورت غیر امن (Insecure deletion of data)

امنیت داده در رایانش ابری

رمز گذاری جستجوپذیر متقارن

رمز گذاری جستجوپذیر نامتقارن

رمز گذاری تمام هم ریخت

برون سپاری امن پایگاه داده و

رویکردهای تامین محرمانگی

وارسی صحت پاسخ پرسمان روی

پایگاه داده برون سپاری شده

روشهای ذخیره سازی داده های

رمز شده غیر تکراری در ابر

مروری بر محصولات موجود

در زمینه برون سپاری امن داده

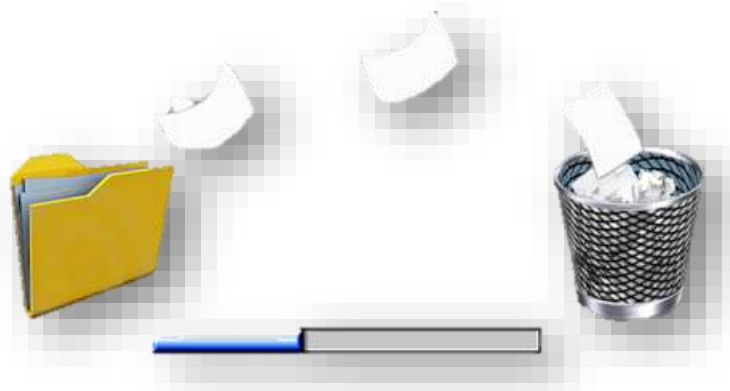
امنیت داده و مدیریت مخاطرات

در رایانش ابری

□ مثال:

- درخواست حذف ماشین مجازی
- درخواست حذف فایل
- درخواست حذف ایمیل / فکس / ...
- جابجا شدن منابع در نتیجه مقیاس پذیری خدمت

□ زمانی اتفاق می افتد که داده ها به طور کامل حذف نشوند و امکان بازیابی آنها وجود داشته باشد.
(نظیر حذف منطقی، حذف از روی دیسک، حذف کپی پشتیبان)



۱

۲

۳

۴

۵

۶

۷

۸

مخاطره حملات منع خدمت (DOS)

امنیت داده در رایانش ابری

رمز گذاری جستجوپذیر متقارن

رمز گذاری جستجوپذیر نامتقارن

رمز گذاری تمام هم ریخت

برون سپاری امن پایگاه داده و

رویکردهای تامین محرمانگی

وارسی صحت پاسخ پرسمان روی

پایگاه داده برون سپاری شده

روشهای ذخیره سازی داده های

رمز شده غیر تکراری در ابر

مروری بر محصولات موجود

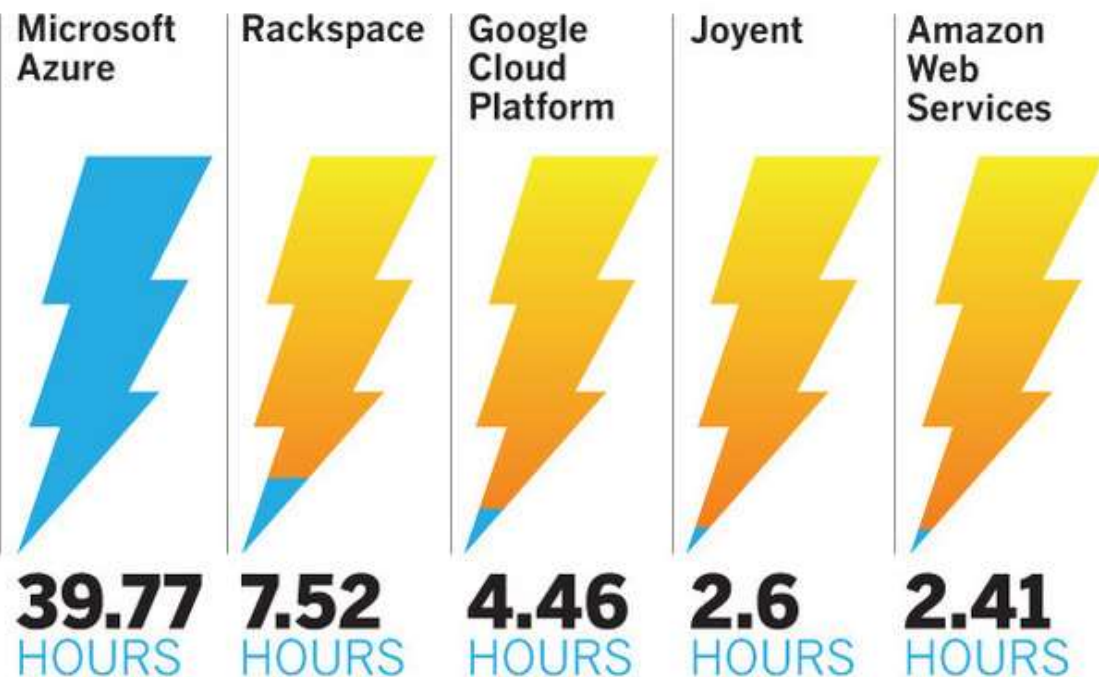
در زمینه برون سپاری امن داده

امنیت داده و مدیریت مخاطرات

در رایانش ابری

How reliable is the cloud?

Downtime in 2014 of compute services (in hours)



SOURCE: CLOUDHARMONY

Availability	Total downtime (HH:MM:SS)		
	Per day	Per month	Per year
99.999%	00:00:00.4	00:00:26	00:05:15
99.99%	00:00:08	00:04:22	00:52:35
99.9%	00:01:26	00:43:49	08:45:56
99%	00:14:23	07:18:17	87:39:29

۱

۲

۳

۴

۵

۶

۷

۸

مخاطره حملات منع خدمت (DOS)

امنیت داده در رایانش ابری

رمز گذاری جستجوپذیر متقارن

رمز گذاری جستجوپذیر نامتقارن

رمز گذاری تمام هم ریخت

برون سپاری امن پایگاه داده و

رویکردهای تامین محرمانگی

وارسی صحت پاسخ پرسمان روی

پایگاه داده برون سپاری شده

روشهای ذخیره سازی داده های

رمز شده غیر تکراری در ابر

مروری بر محصولات موجود

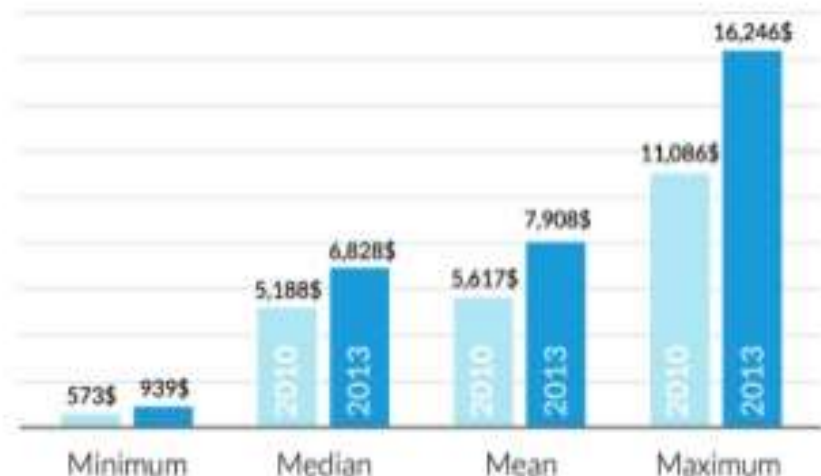
در زمینه برون سپاری امن داده

امنیت داده و مدیریت مخاطرات

در رایانش ابری

On average, the cost of an unplanned outage per minute is likely to reach almost **\$8,000 per incident**

Total cost per minute of an unplanned outage



□ زمانی اتفاق می افتد که سامانه اشباع شود.
(نتواند پاسخگو باشد)

□ مثال:

- بوق اشغال برای دریافت فکس ابری
- قطع شدن خدمت بخاطر ترافیک بالا

مخاطره از دست رفتن کلیدهای رمزنگاشتی (Loss of Cryptographic Keys)

امنیت داده در رایانش ابری

رمز گذاری جستجوپذیر متقارن

رمز گذاری جستجوپذیر نامتقارن

رمز گذاری تمام هم ریخت

برون سپاری امن پایگاه داده و

رویکردهای تامین محرمانگی

وارسی صحت پاسخ پرسمان روی

پایگاه داده برون سپاری شده

روشهای ذخیره سازی داده های

رمز شده غیر تکراری در ابر

مروری بر محصولات موجود

در زمینه برون سپاری امن داده

امنیت داده و مدیریت مخاطرات

در رایانش ابری

□ مثال:

- کلید های SSL
- کلیدهای رمزنگاشتی فایل
- کلیدهای دسترسی به ماشین
- فراموشی رمز عبور



۱

۲

۳

۴

۵

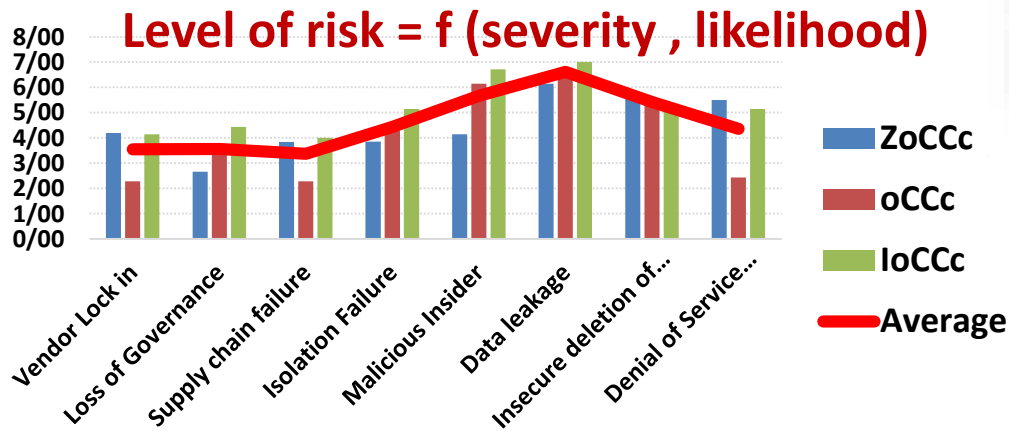
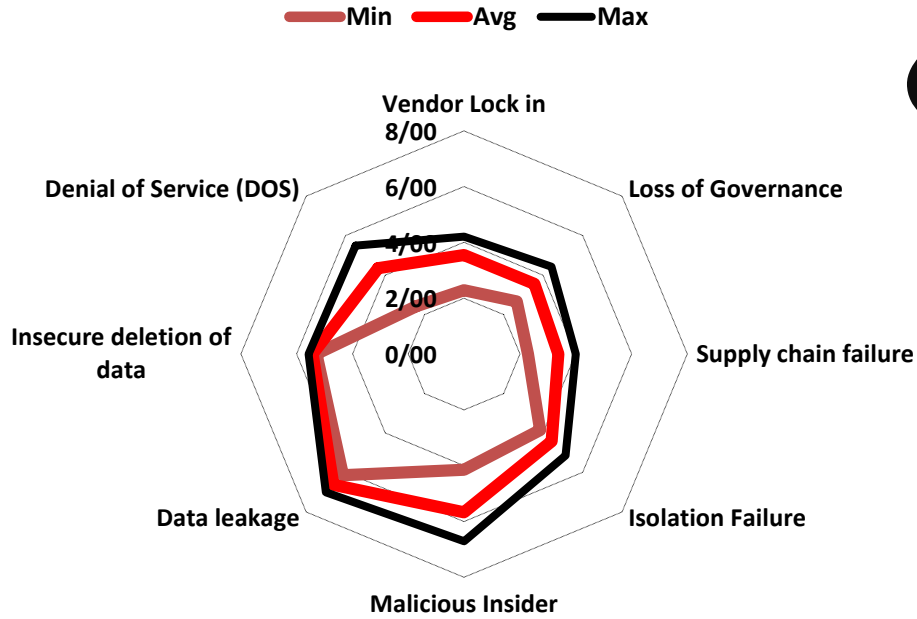
۶

۷

۸

مثالی از تحلیل مخاطرات در سرویس های ابری

(بررسی موردی فکس ابری در سه جامعه کاربری)



امنیت داده در رایانش ابری

رمز گذاری جستجوپذیر نامتقارن

رمز گذاری جستجوپذیر نامتقارن

رمز گذاری تمام هم ریخت

برون سپاری امن پایگاه داده و

رویکردهای تامین محرمانگی

وارسی صحت پاسخ پرمسان روی

پایگاه داده برون سپاری شده

روشهای ذخیره سازی داده های

رمز شده غیر تکراری در ابر

مروری بر محصولات موجود

در زمینه برون سپاری امن داده

امنیت داده و مدیریت مخاطرات

در رایانش ابری

مدیریت مخاطرات حریم خصوصی

PII : Personally Identifiable Information

PIA: Privacy Impact Assessment (Tools)



Impact	Probability				
	A	B	C	D	E
5					
4					
3					
2					
1					

Risk Probability and Impact Assessment

Probability A - Rare, B - Unlikely, C - Possible, D - likely, E - Frequent
Impact 1= up to \$100K, 2= up to \$1M, 3= up to \$5M, 4= up to \$10M, 5= >\$10M

امنیت داده در رایانش ابری

رمز گذاری جستجوپذیر متقارن

رمز گذاری جستجوپذیر نامتقارن

رمز گذاری تمام هم ریخت

برون سپاری امن پایگاه داده و

رویکردهای تامین محرمانگی

وارسی صحت پاسخ پرسمان روی

پایگاه داده برون سپاری شده

روشهای ذخیره سازی داده های

رمز شده غیر تکراری در ابر

مروری بر محصولات موجود

در زمینه برون سپاری امن داده

امنیت داده و مدیریت مخاطرات

در رایانش ابری

امنیت داده در رایانش ابری

رمز گذاری جستجوپذیر متقارن

رمز گذاری جستجوپذیر نامتقارن

رمز گذاری تمام همریخت

برون سپاری امن پایگاه داده و

رویکردهای تامین محرمانگی

وارسی صحت پاسخ پرسمان روی

پایگاه داده برون سپاری شده

روشهای ذخیره سازی داده های

رمز شده غیر تکراری در ابر

مروری بر محصولات موجود

در زمینه برون سپاری امن داده

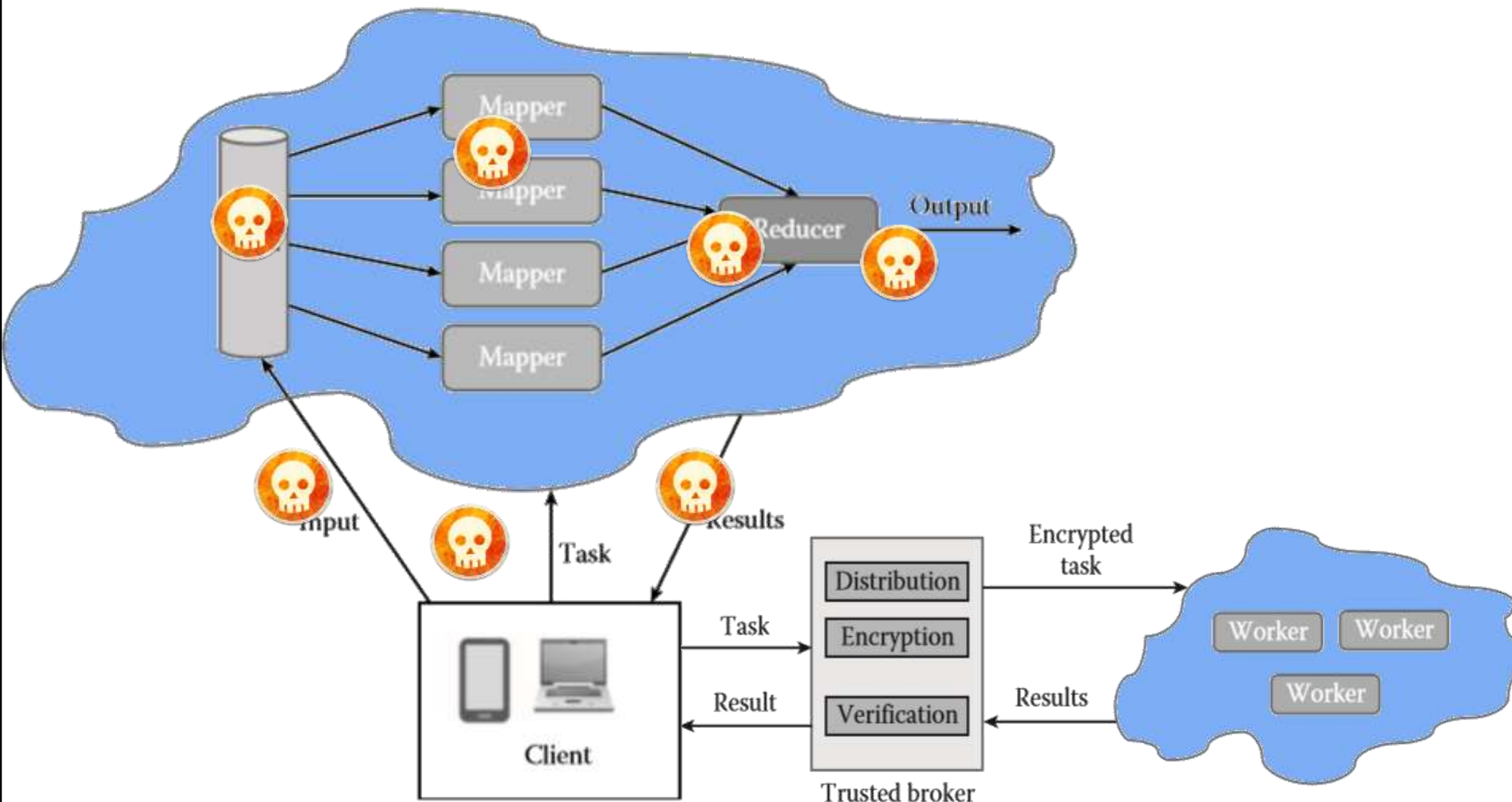
امنیت داده و مدیریت مخاطرات

در رایانش ابری

جمع بندی

بده بستان کار آیی و امنیت
نمایش نهایی!

بده بستان کارآیی و امنیت



امنیت داده در رایانش ابری

رمز گذاری جستجوپذیر متقارن

رمز گذاری جستجوپذیر نامتقارن

رمز گذاری تمام هم ریخت

برون سپاری امن پایگاه داده و

رویکردهای تامین محرمانگی

وارسی صحت پاسخ پرسمان روی

پایگاه داده برون سپاری شده

روشهای ذخیره سازی داده های

رمز شده غیر تکراری در ابر

مروری بر محصولات موجود

در زمینه برون سپاری امن داده

امنیت داده و مدیریت مخاطرات

در رایانش ابری

بده بستان کارآیی و امنیت

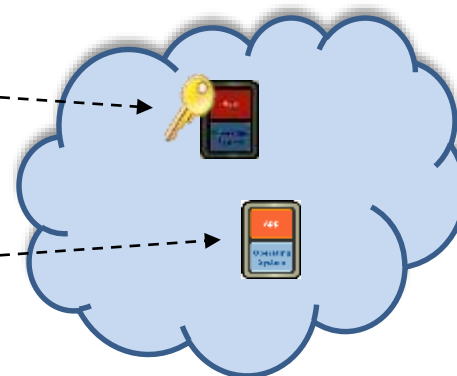
```

response time:
  min:          9220.97ms
  avg:          9848.48ms
  max:          28314.09ms

```

پرسمان بر
روی داده های
رمز شده

Select * from table_cipher



Select * from table_plain

```

response time:
  min:          5.10ms
  avg:          6.81ms
  max:          15.14ms

```

پرسمان بر
روی داده های
اصلی (غیررمز)

امنیت داده در رایانش ابری

رمز گذاری جستجوپذیر متقارن

رمز گذاری جستجوپذیر نامتقارن

رمز گذاری تمام همریخت

برون سپاری امن پایگاه داده و

رویکردهای تامین محرمانگی

وارسی صحت پاسخ پرسمان روی

پایگاه داده برون سپاری شده

روشهای ذخیره سازی داده های

رمز شده غیر تکراری در ابر

مروری بر محصولات موجود

در زمینه برون سپاری امن داده

امنیت داده و مدیریت مخاطرات

در رایانش ابری

نمایش



امنیت داده در رایانش ابری

رمز گذاری جستجوپذیر متقارن

رمز گذاری جستجوپذیر نامتقارن

رمز گذاری تمام هم ریخت

برون سپاری امن پایگاه داده و

رویکردهای تامین محرمانگی

وارسی صحت پاسخ پرسمان روی

پایگاه داده برون سپاری شده

روشهای ذخیره سازی داده های

رمز شده غیر تکراری در ابر

مروری بر محصولات موجود

در زمینه برون سپاری امن داده

امنیت داده و مدیریت مخاطرات

در رایانش ابری

باتشکر از توجه شما



امنیت داده در رایانش ابری

رمز گذاری جستجوپذیر متقارن

رمز گذاری جستجوپذیر نامتقارن

رمز گذاری تمام همریخت

برون سپاری امن پایگاه داده و

رویکردهای تامین محرمانگی

وارسی صحت پاسخ پرسمان روی

پایگاه داده برون سپاری شده

روشهای ذخیره سازی داده های

رمز شده غیر تکراری در ابر

مروری بر محصولات موجود

در زمینه برون سپاری امن داده

امنیت داده و مدیریت مخاطرات

در رایانش ابری