کارگاه عملی امنیت داده و مدیریت مخاطرات در رایانش ابری

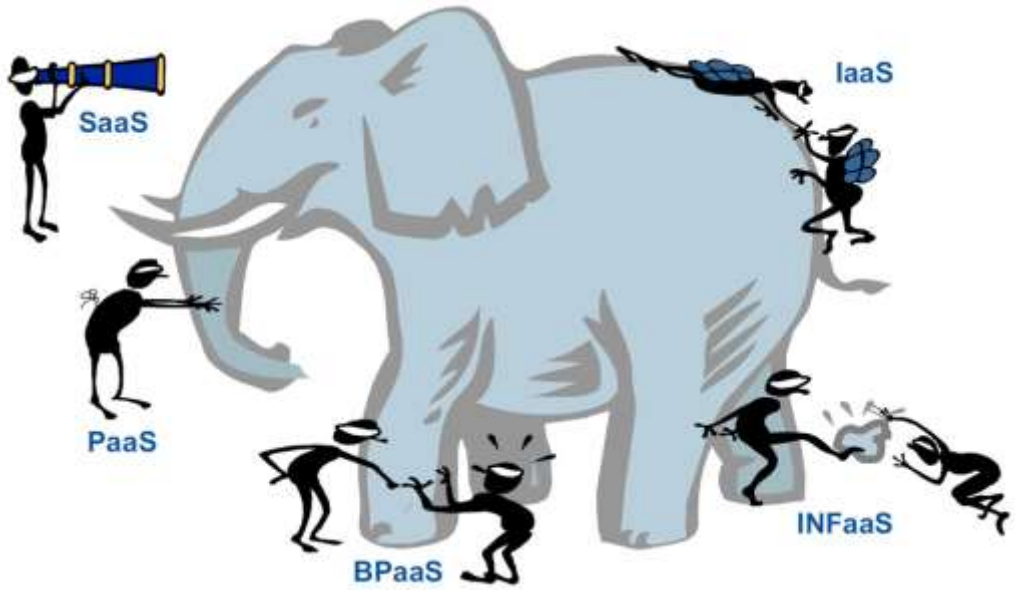
مرتضی سرگلزایی جوان

مسئول مرکز تحقیقات رایانش ابری
موسس جامعه آزاد رایانش ابری ایران
www.msjavan.ir
@msjavan_ir

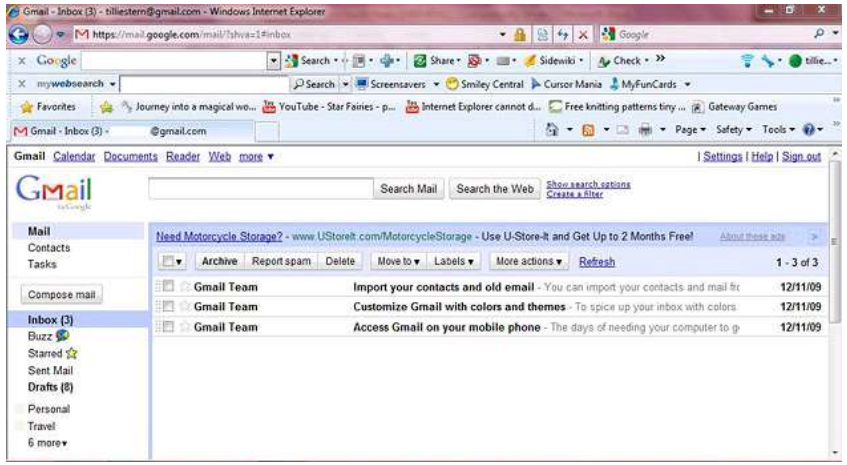
چشم‌انداز

- مقدمه
  - مروری بر رایانش ابری با مثال های عملی
  - خدمات رایانش ابری در ایران
- مدیریت مخاطرات
  - مفاهیم پایه و چهارچوب ارزیابی
  - مطالعه موردی (کارگاه عملی)
- نتیجه گیری
  - بده بستان امنیت و کارآیی
  - نمایش نهایی!

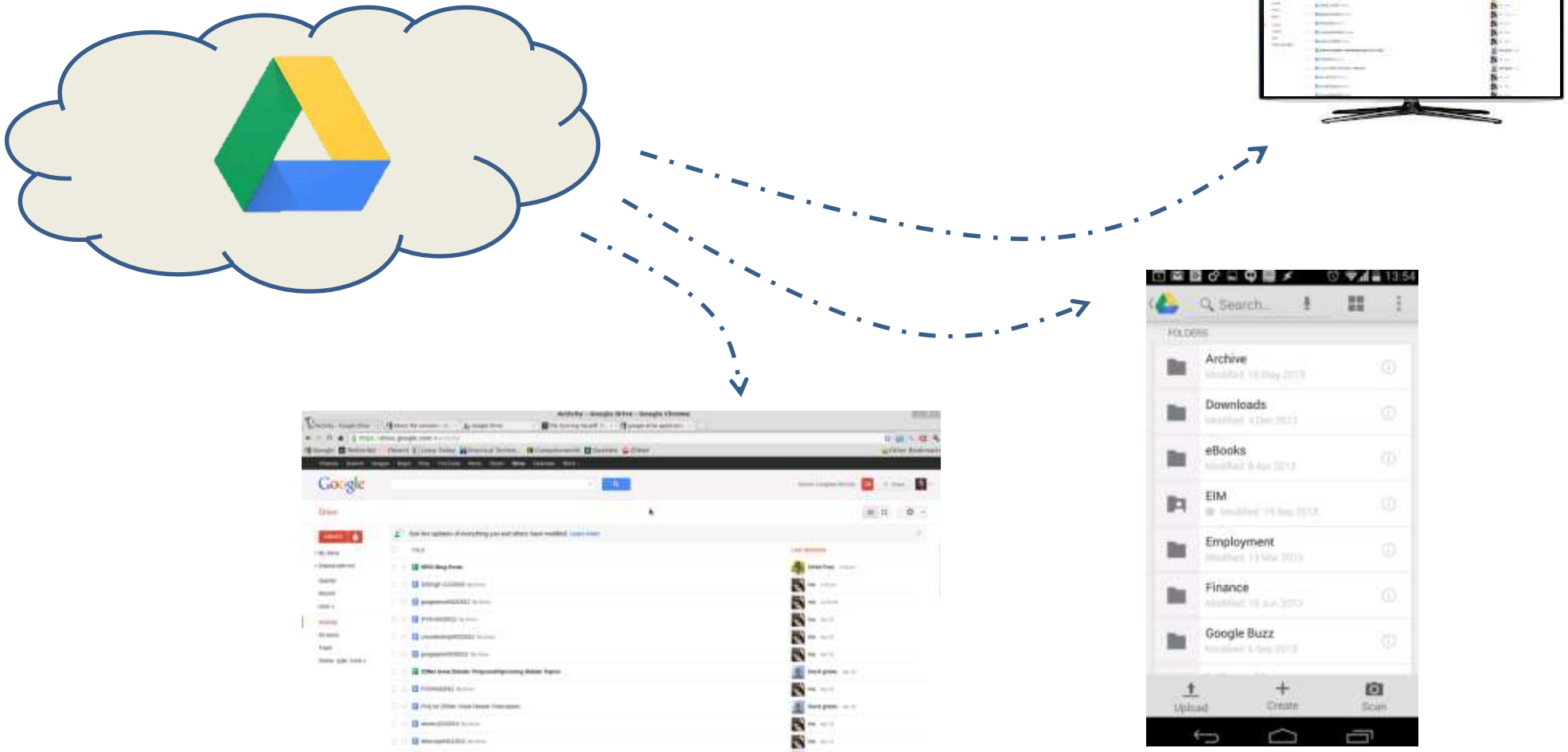
مقدمه



مثال موردی : Email

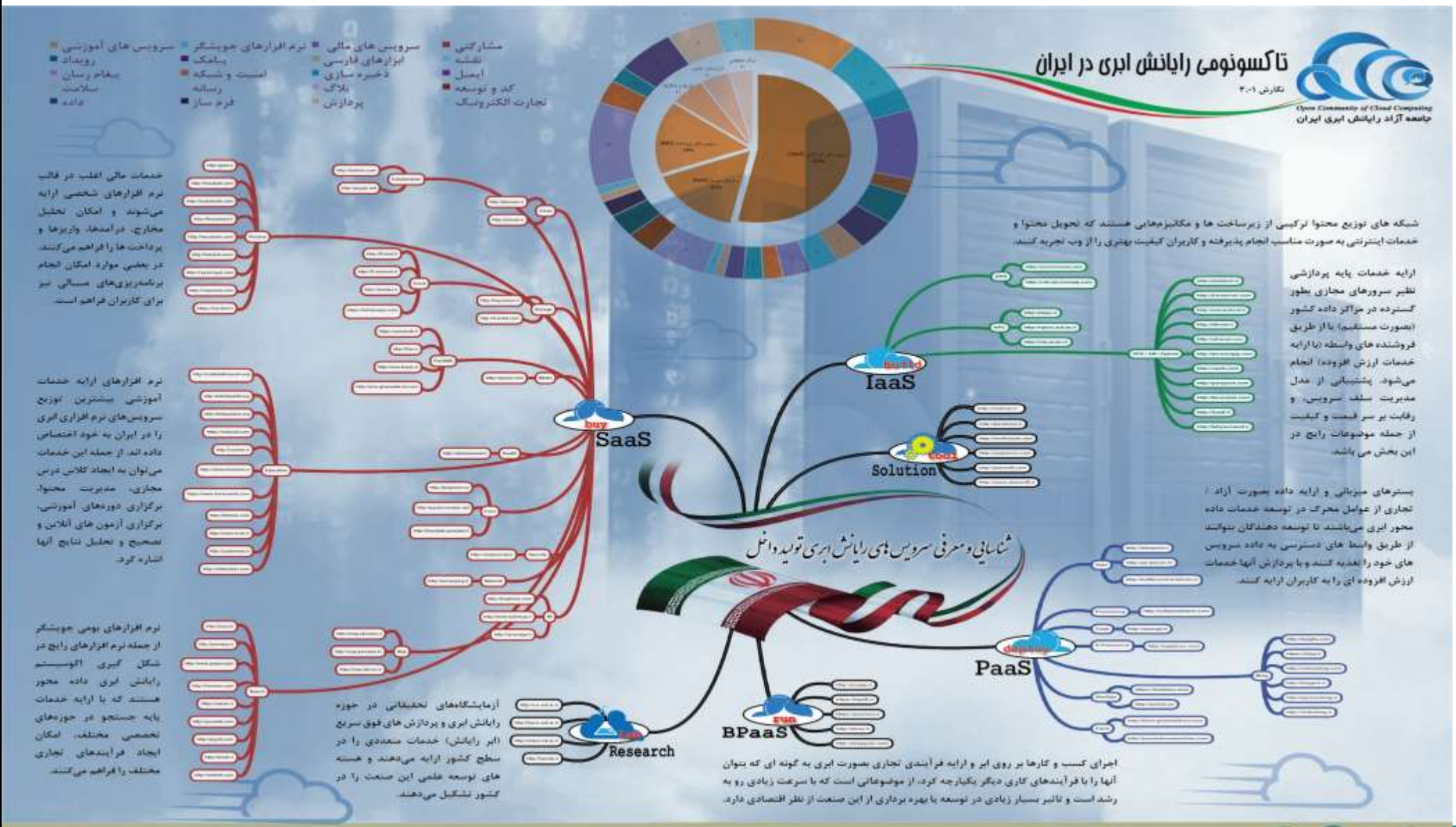


مثال موردی : Drive



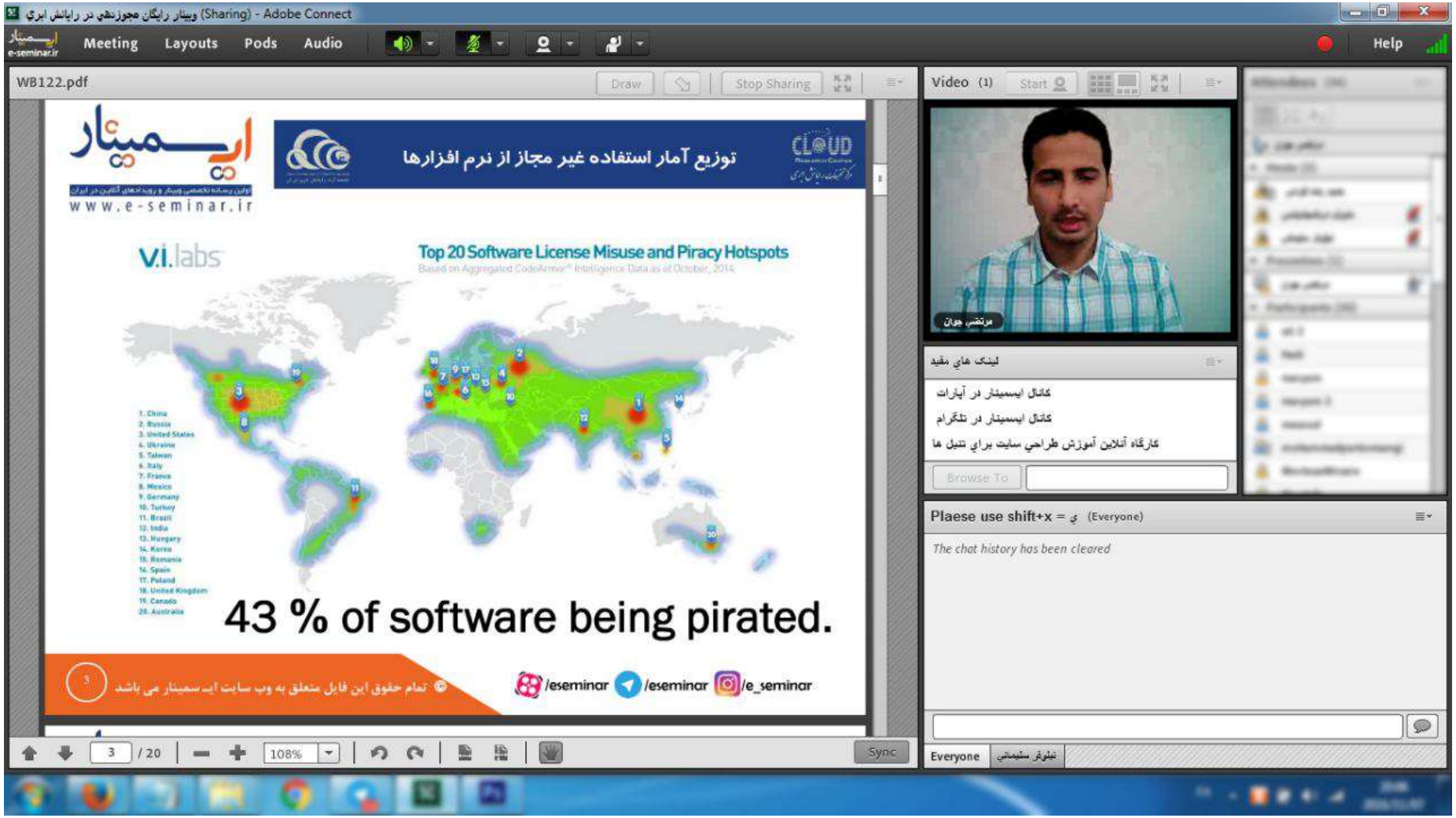
مثال موردی : Office

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



مدیریت رویدادها به صورت برخط

برگزاری کنفرانس و همایش به صورت برخط

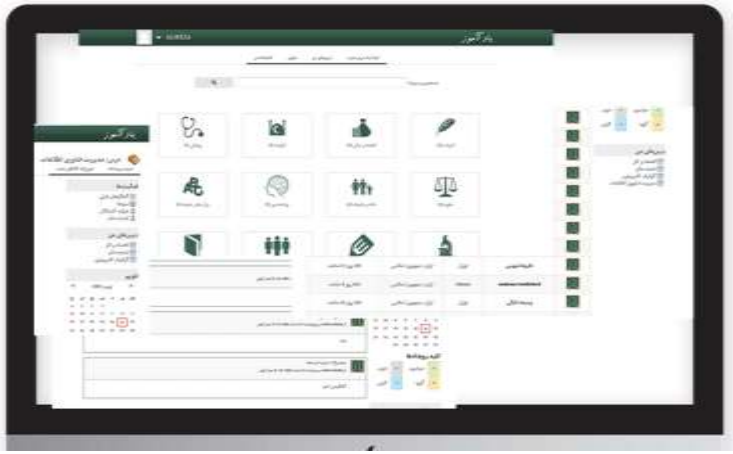


کلاس درس برخط

کلاس درس خود را به اینترنت بیاورید!

اگر در دانشگاه تدریس می کنید، اگر تدریسیار 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!

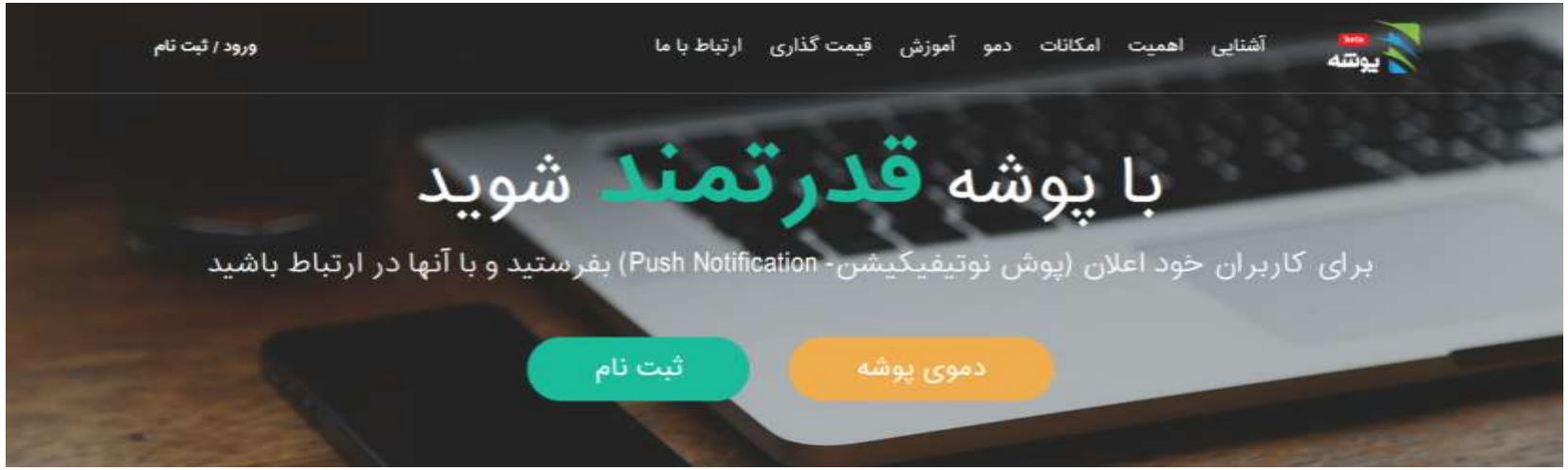
امکاناتی از قبیل تحویل و دریافت تمرینات و نمرات آن ها از طریق اینترنت، نمره دهی به دانشجویان، پرسش و پاسخ اینترنتی در کلاس، امکان آپلود فایل، عکس و فیلم؛ باعث می شود تا مدیریت کلاس شما بسیار راحت تر، مفیدتر و جذاب تر گردد.



سیستم حسابداری شخصی

ارسال فکس برخط

ابزارهای توسعه همراه و تارنما

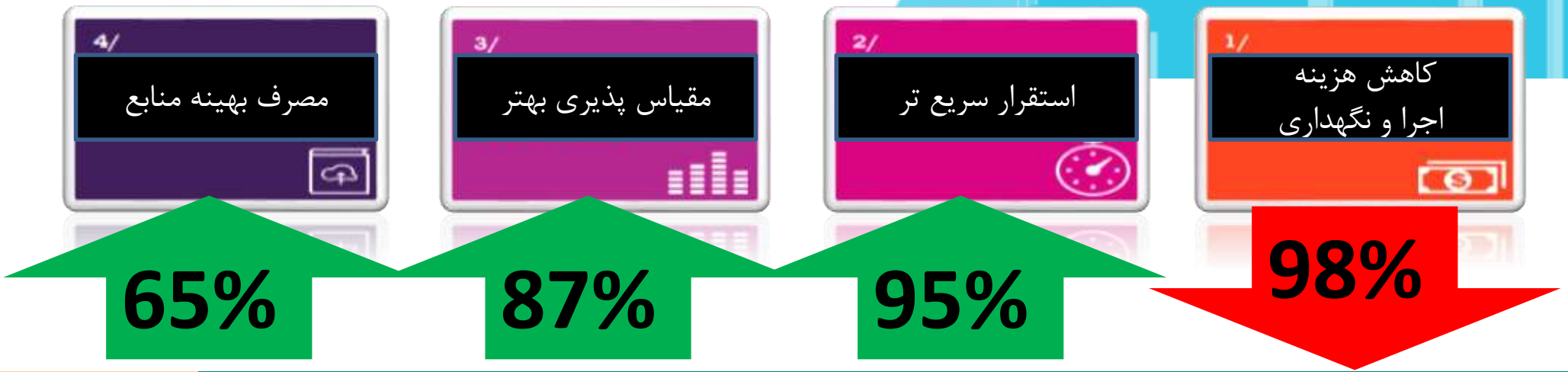


مزایای اتصال به شبکه رایانش ...

تا ۲۰۲۰

۹۴ درصد سازمان ها و شرکت ها

به زیرساخت های ابری متصل می شوند



مخاطرات استفاده از شبکه های مختلف چیست؟

شبکه برق

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

شبکه آب

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

شبکه تلفن

قطع شدن تلفن
شنود مکالمات

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

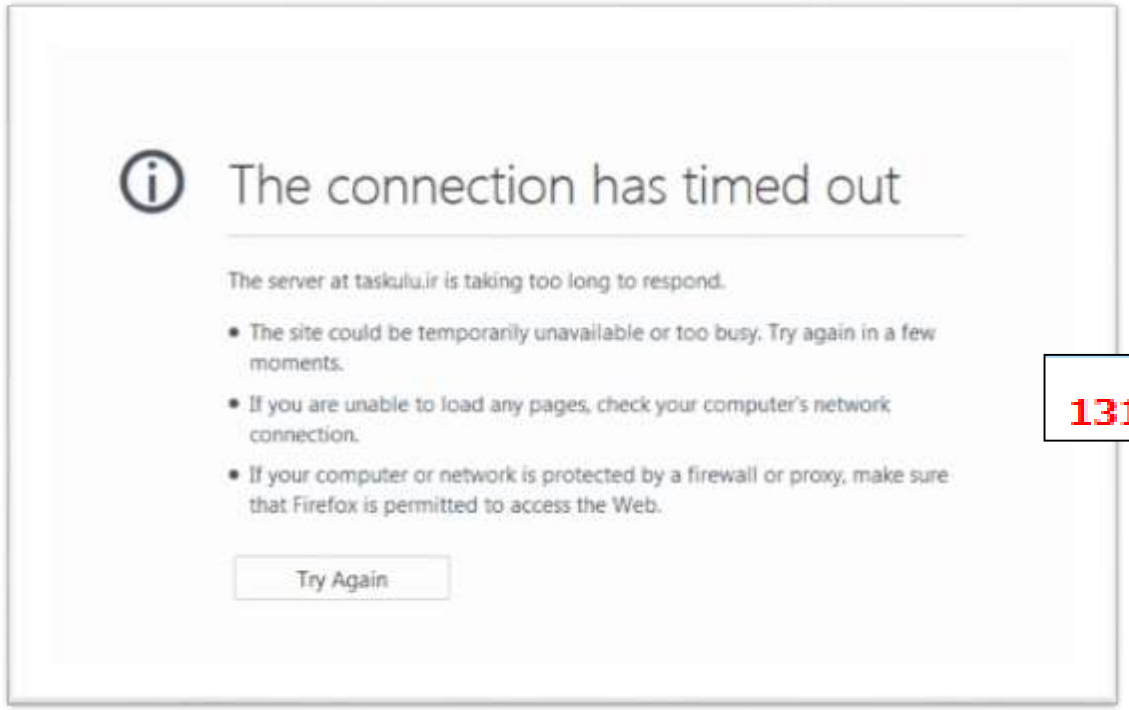
طی ۱۵ الی ۲۰ سال آینده، استفاده از فناوری اطلاعات آنچنان **فراگیر** می شود که اتصال به **شبکه رایانش** یک نیاز همگانی خواهد بود.

شبکه برق

شبکه آب

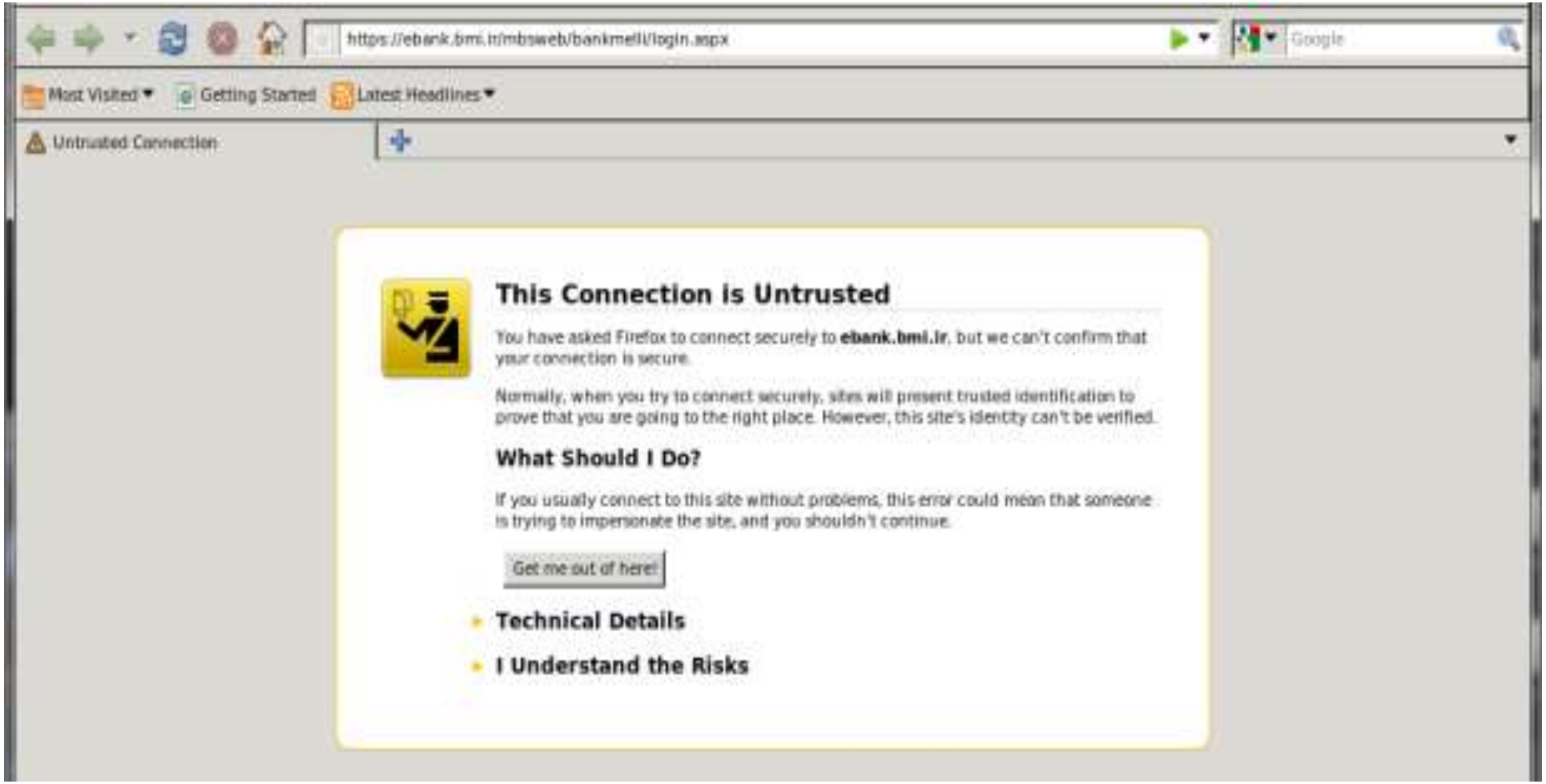
شبکه تلفن

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



پرداخت موفقیت آمیز نبود. کد خطا: 131

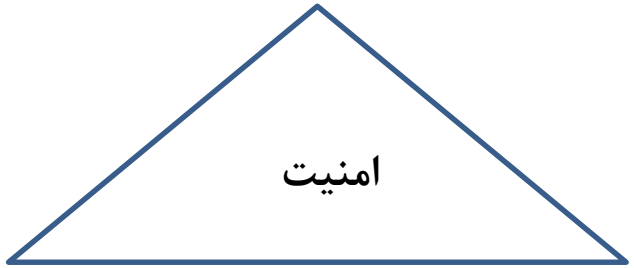
آیا با مشکل عدم اعتماد به گواهینامه یک منزلگاه اینترنتی مواجه شده اید؟



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

مدیریت مخاطرات

امنیت نرم
(حریم خصوصی، اعتماد، شهرت، کلان داده و ...)

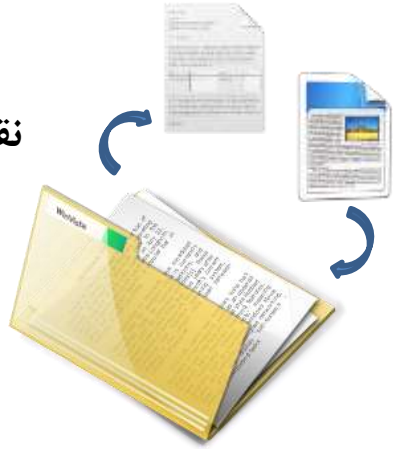


تئوری و رمز
(رمزنگاری متقارن، نامتقارن و ...)

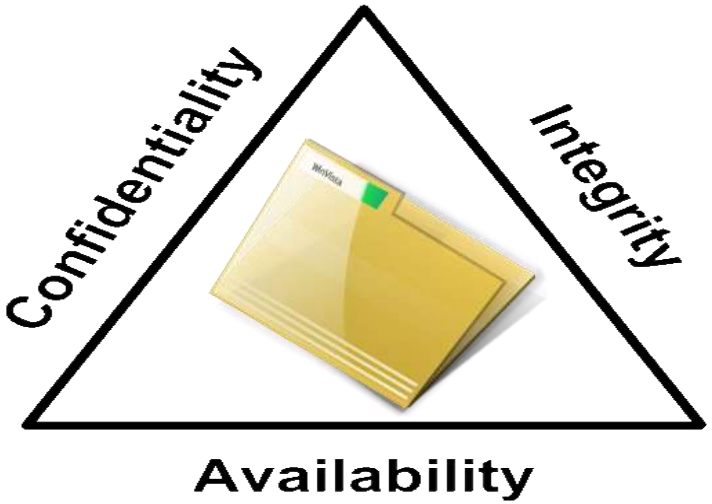
مهندسی و شبکه
(دیوار آتش، ضد ویروس و ...)

ابعاد مخاطرات امنیتی (مثال)

نقض صحت داده



نقض محرمانگی داده

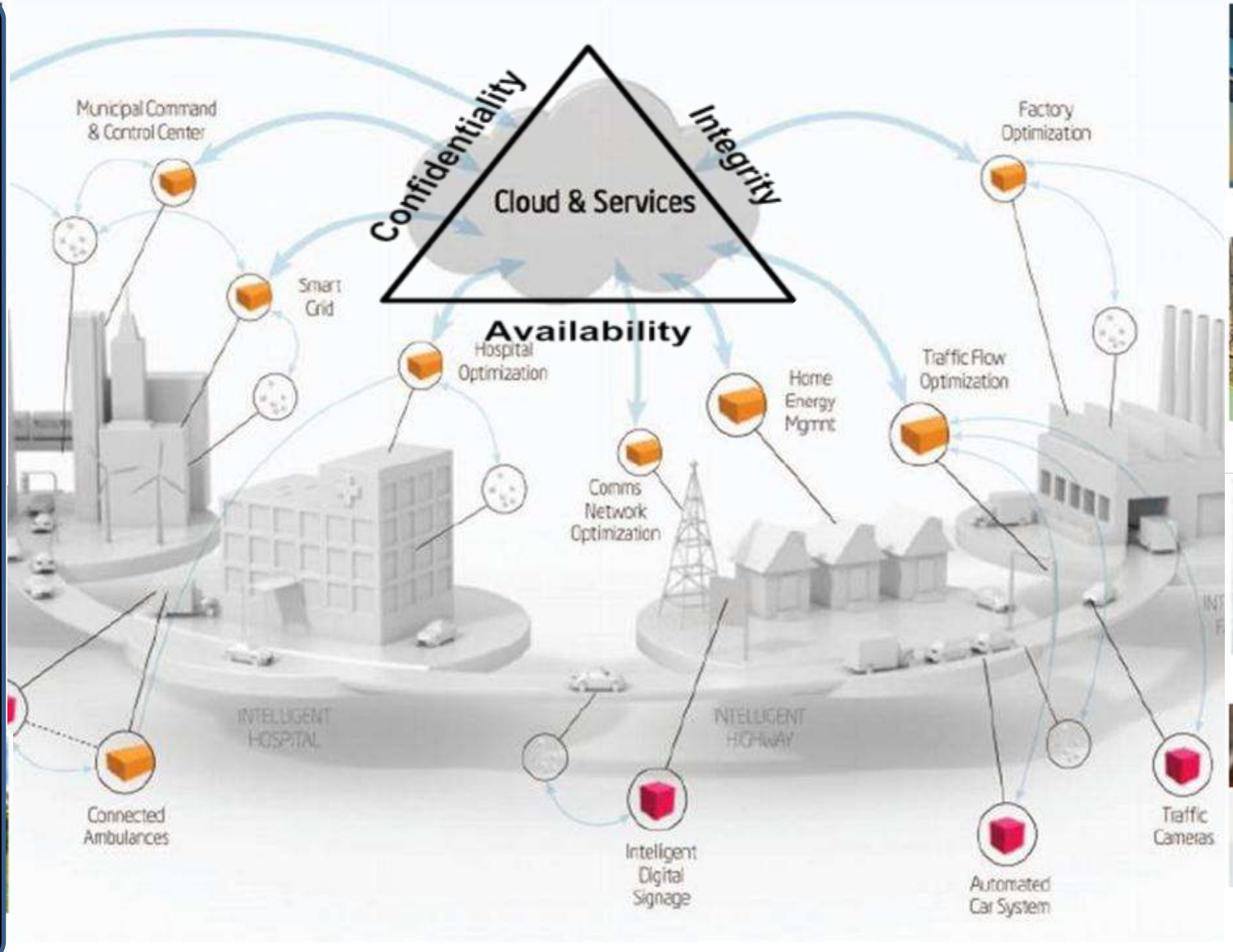


از دسترس خارج شدن داده

نمایش

رایانش ابری: صنعت همگانی پنجم ...

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



Smart Oil

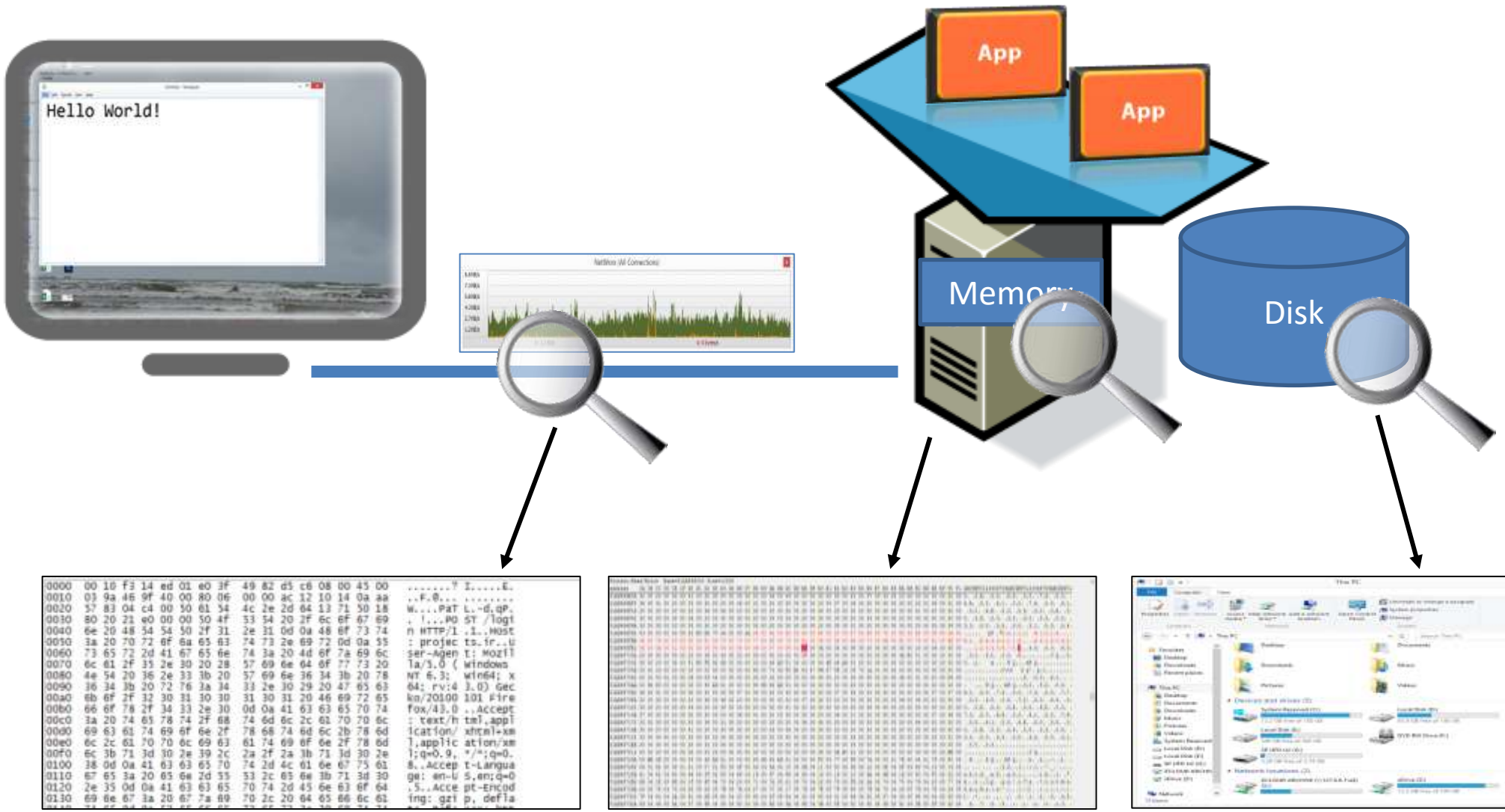
Smart logistics

Smart consumer products

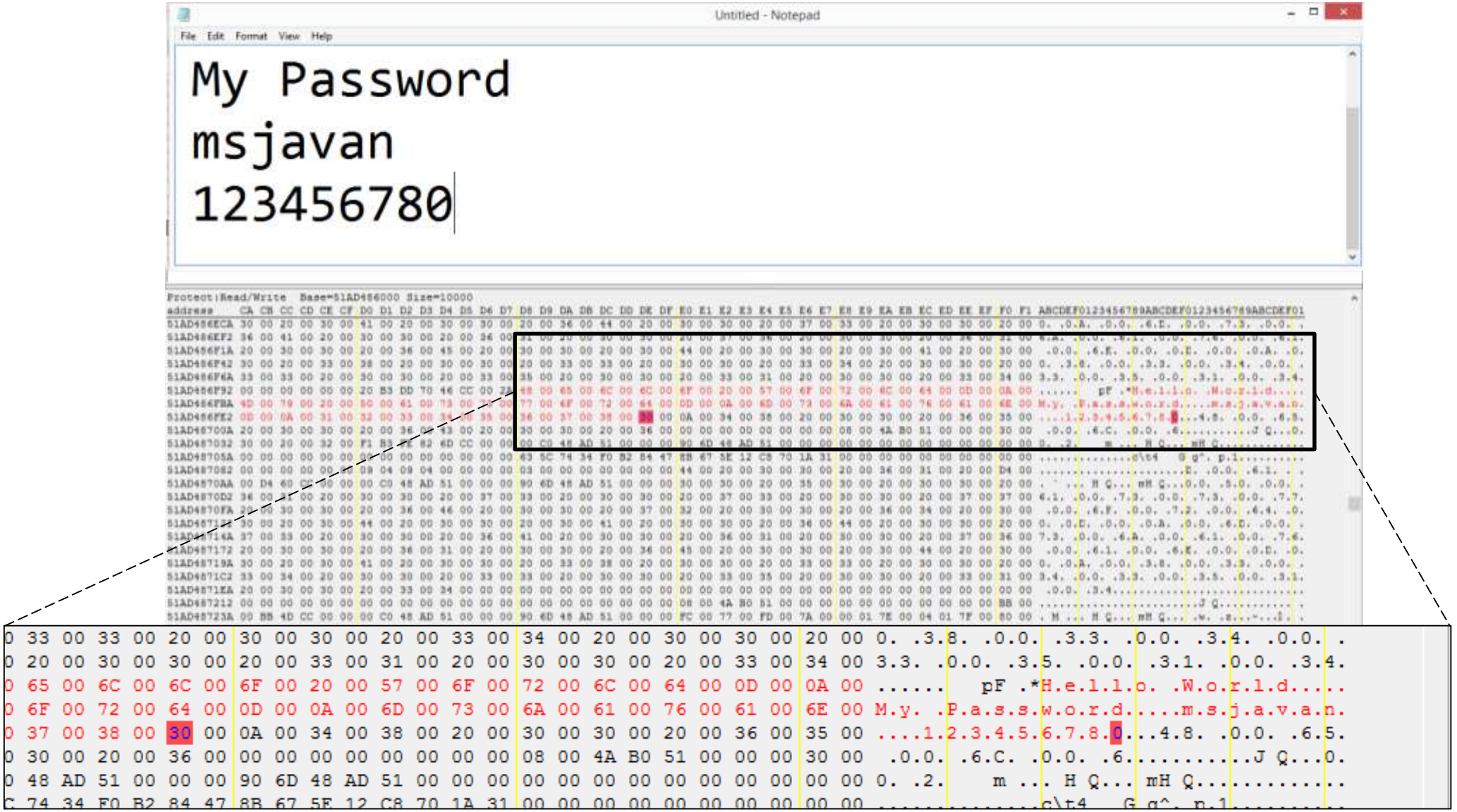
Smart banking

مثال:

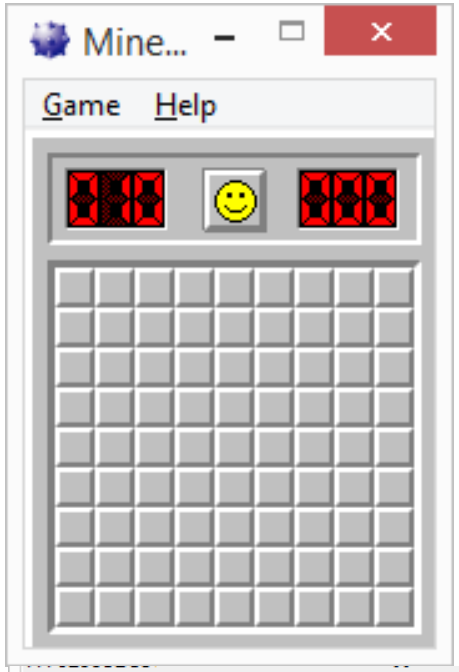
انواع داده: (ثابت / در حرکت / در حال استفاده)



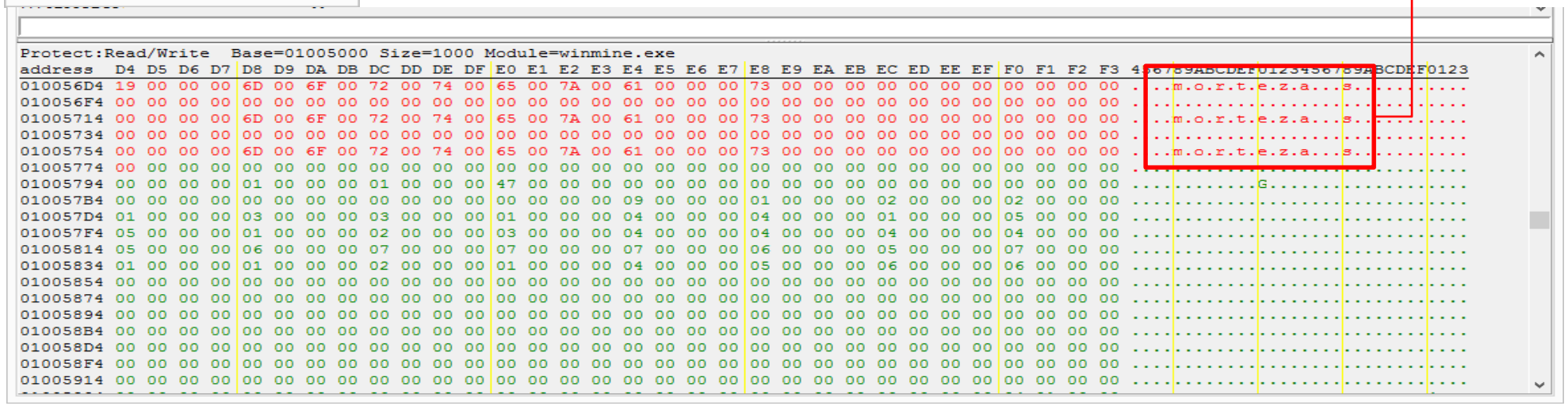
مثال: (نقض محرمانگی و صحت)



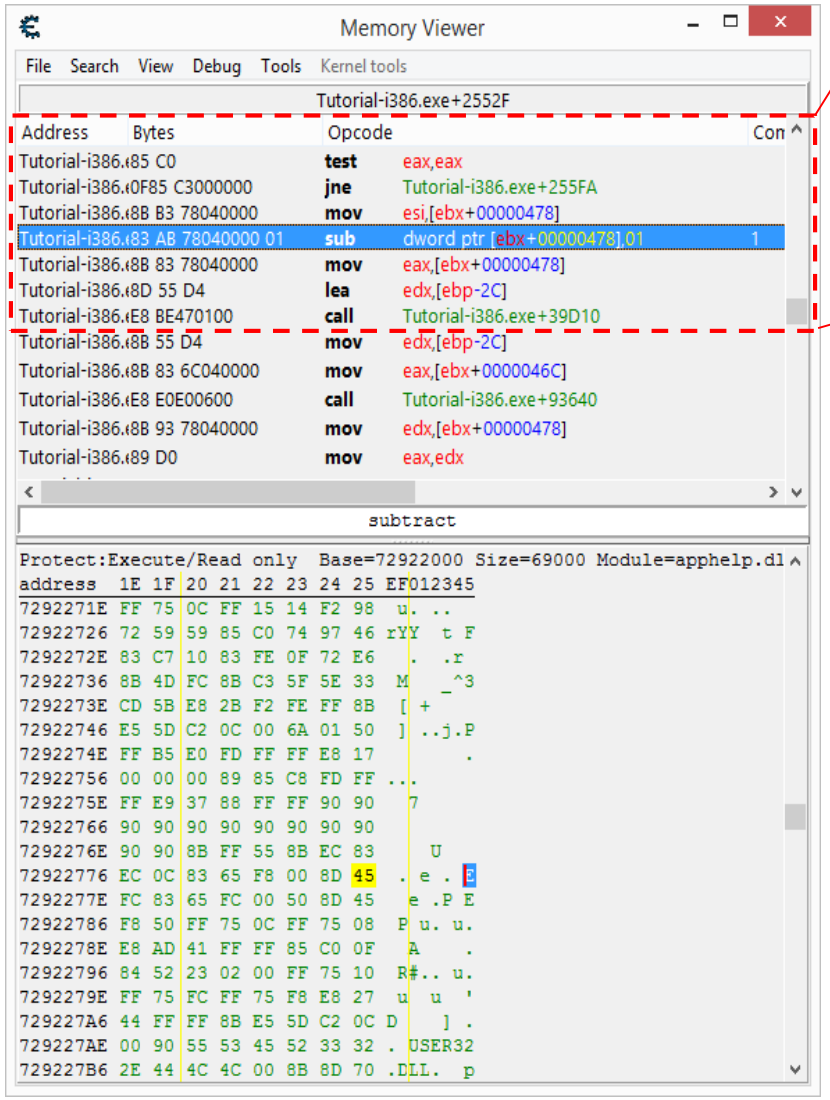
مثال: (نقض محرمانگی و صحت)



نقض صحت و
نقض محرمانگی



مثال: (نقض صحت)



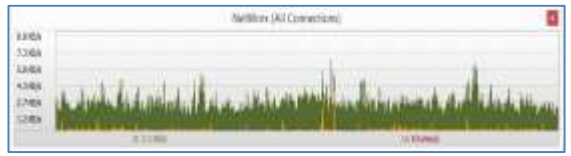
Address	Bytes	Opcode	Con
Tutorial-i386.exe+2552F	85 C0	test	eax,eax
Tutorial-i386.exe+2552F	0F85 C3000000	jne	Tutorial-i386.exe+255FA
Tutorial-i386.exe+2552F	8B B3 78040000	mov	esi,[ebx+00000478]
Tutorial-i386.exe+2552F	83 AB 78040000 01	sub	dword ptr [ebx+00000478],01 1
Tutorial-i386.exe+2552F	8B 83 78040000	mov	eax,[ebx+00000478]
Tutorial-i386.exe+2552F	8D 55 D4	lea	edx,[ebp-2C]
Tutorial-i386.exe+2552F	E8 BE470100	call	Tutorial-i386.exe+39D10

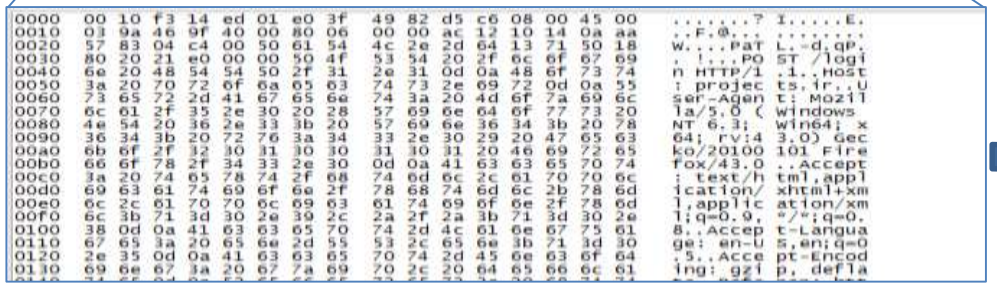
Address	Bytes	Opcode	Con
Tutorial-i386.exe+2552F	85 C0	test	eax,eax
Tutorial-i386.exe+2552F	0F85 C3000000	jne	Tutorial-i386.exe+255FA
Tutorial-i386.exe+2552F	8B B3 78040000	mov	esi,[ebx+00000478]
Tutorial-i386.exe+2552F	E9 BEAA3901	jmp	017C0000
Tutorial-i386.exe+2552F	90	nop	
Tutorial-i386.exe+2552F	90	nop	
Tutorial-i386.exe+2552F	8B 83 78040000	mov	eax,[ebx+00000478]
Tutorial-i386.exe+2552F	8D 55 D4	lea	edx,[ebp-2C]

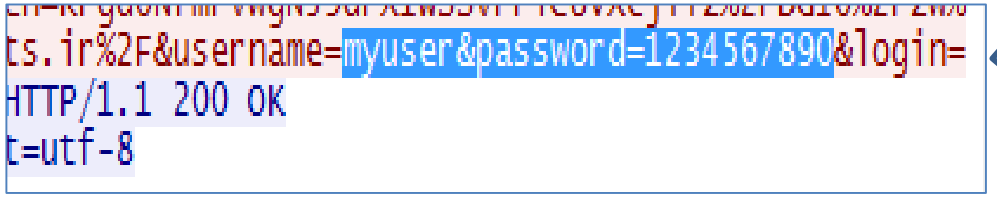
017C0000

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

مثال: (نقض محرمانگی)

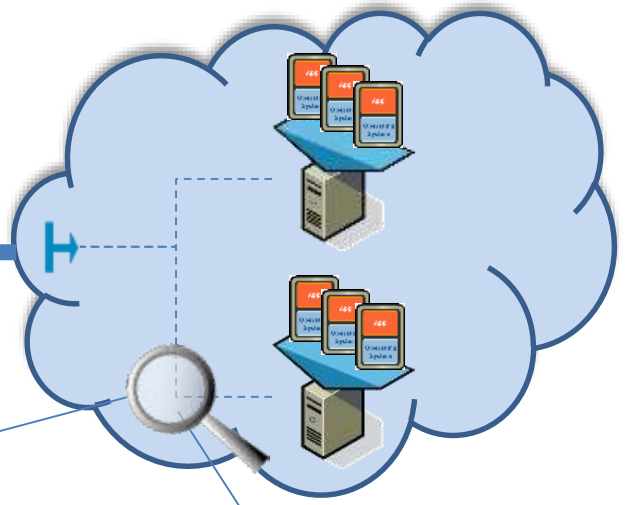


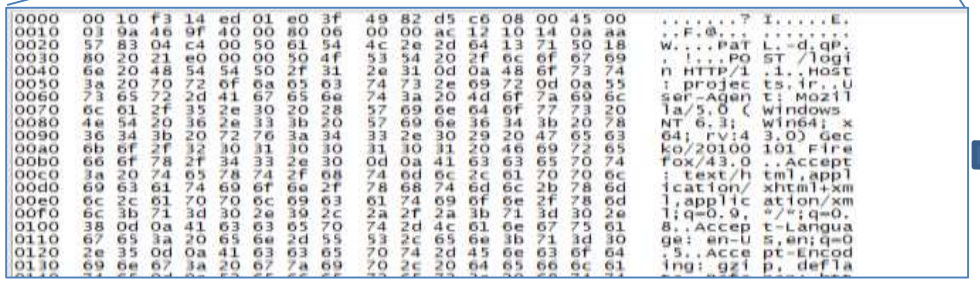




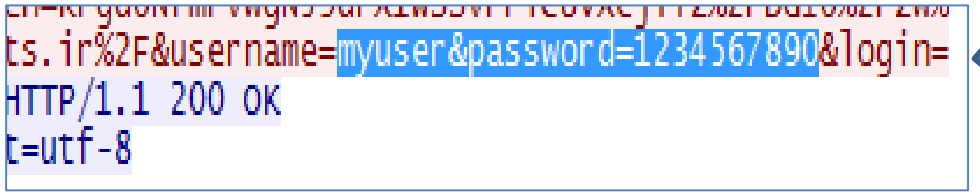
Decode
کدگشایی

مثال: (نقض محرمانگی)

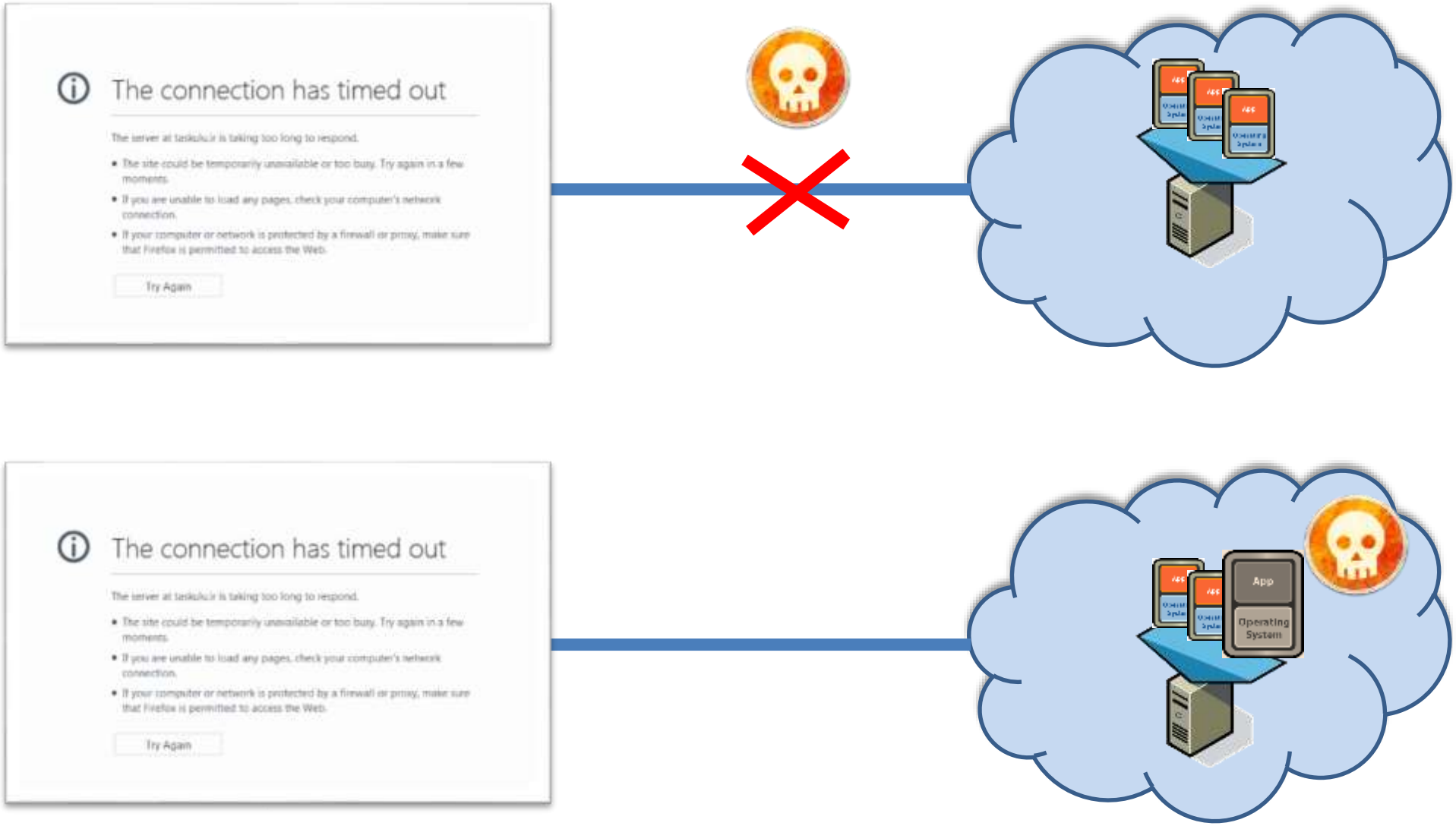




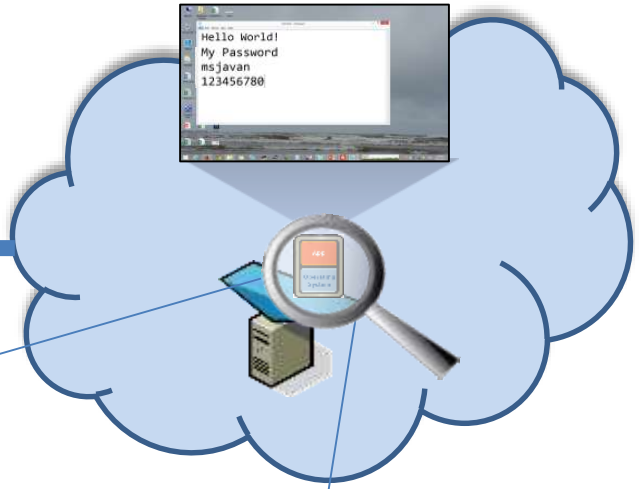
Decode
کدگشایی

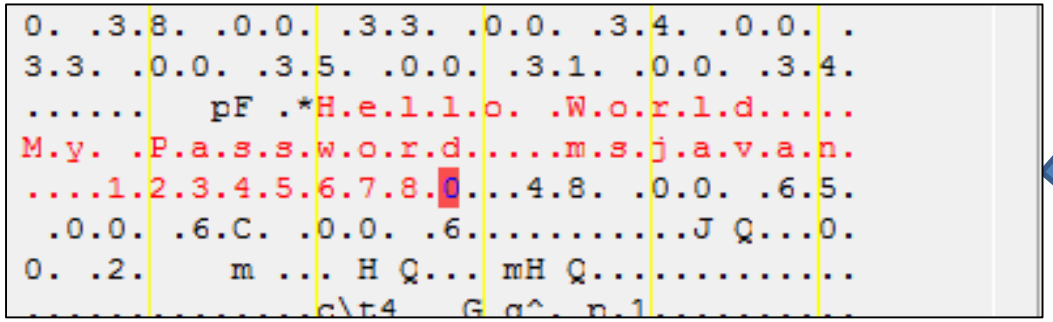


مثال: (نقض دسترسی)



مثال: (نقض محرمانگی و صحت)

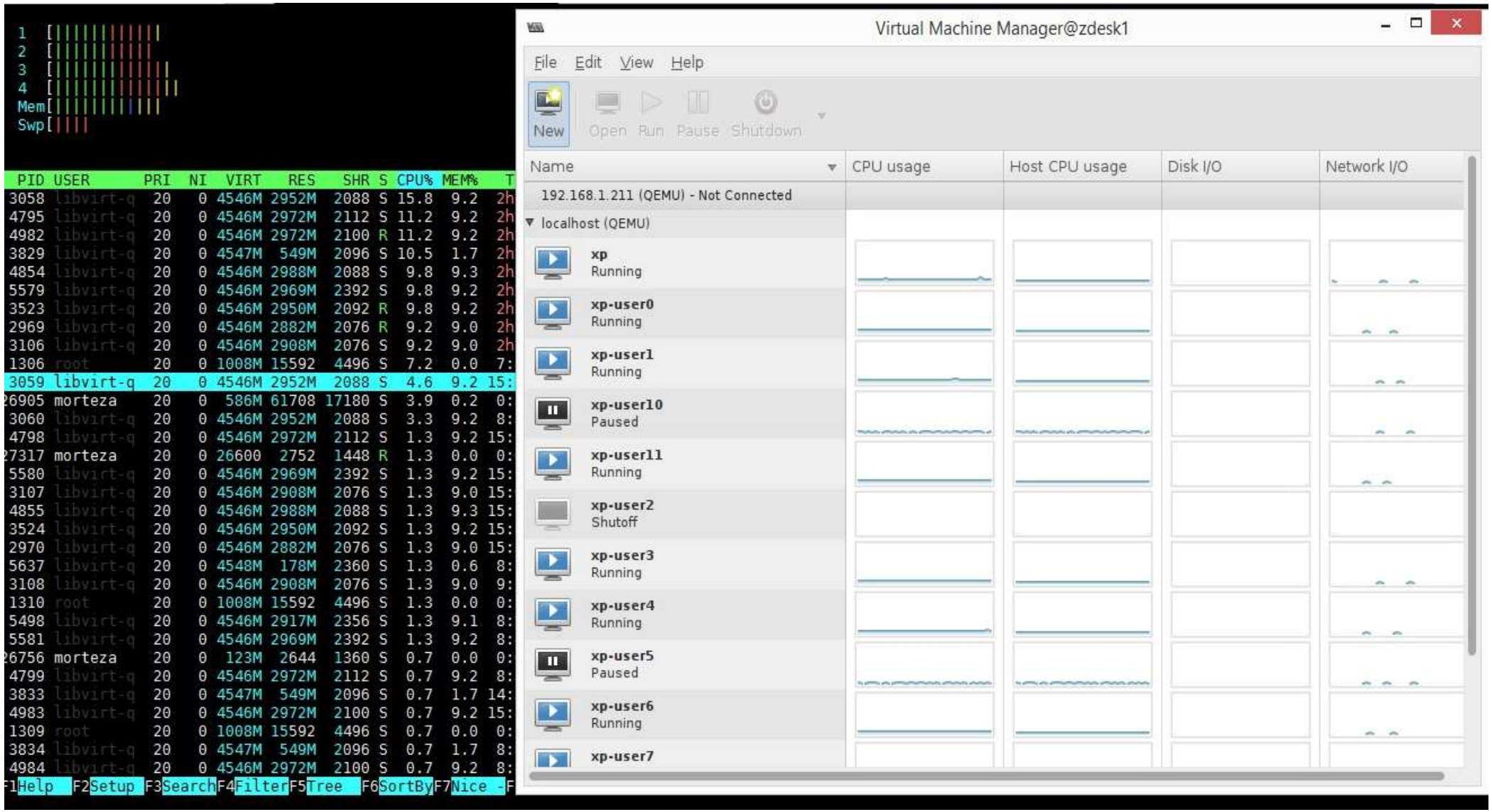




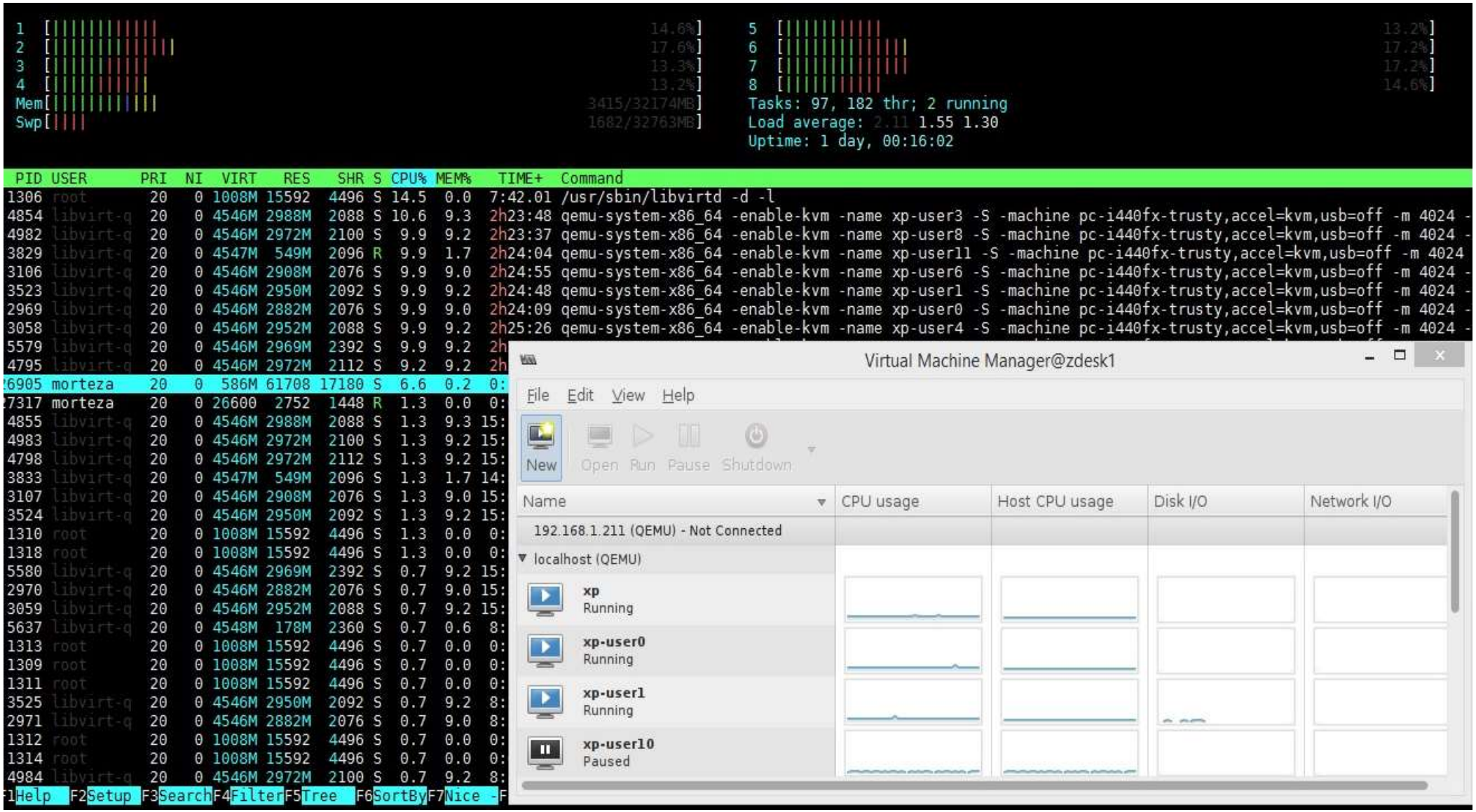
Decode

کدگشایی

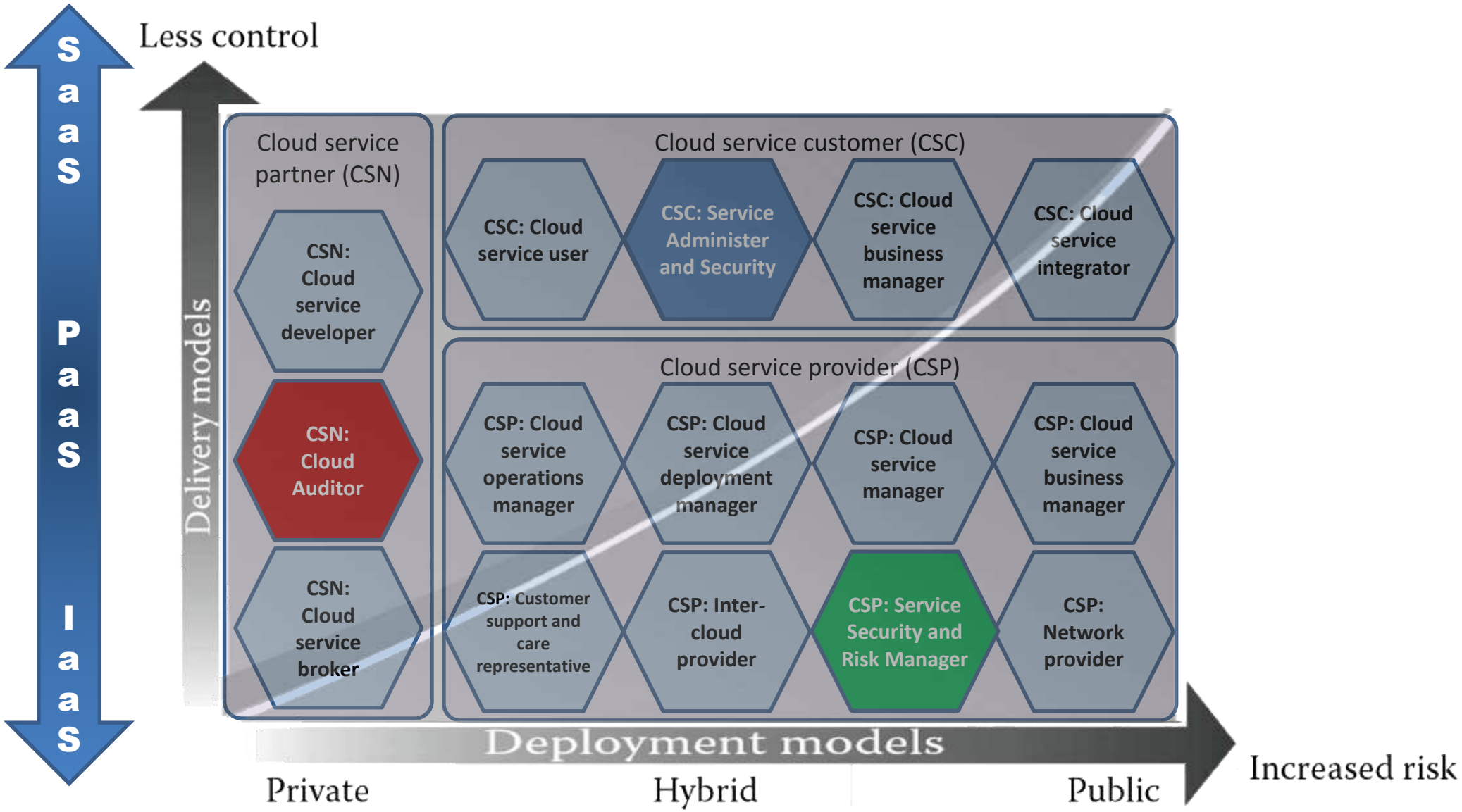
مثال موردی: VDI



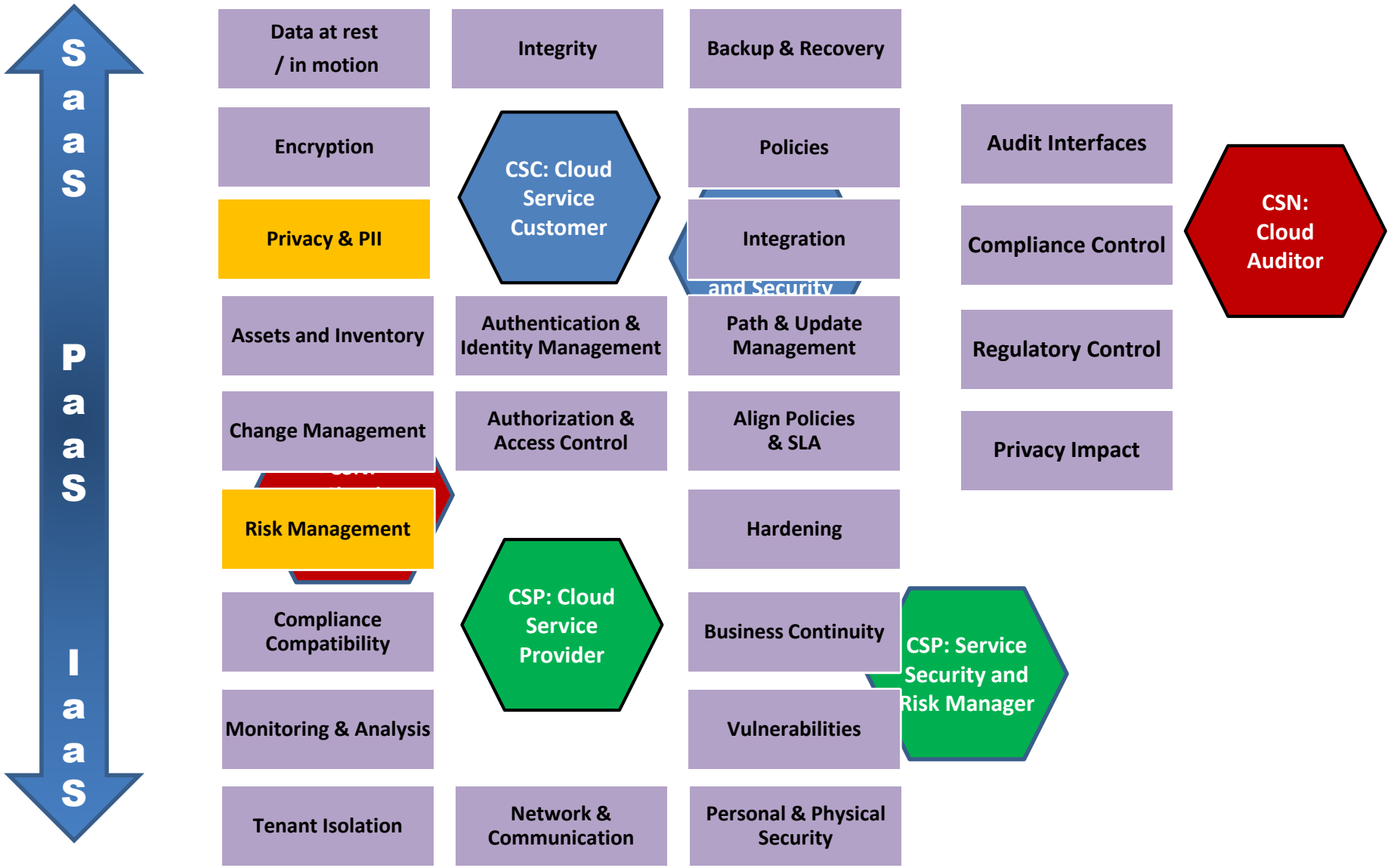
مثال موردی: VDI



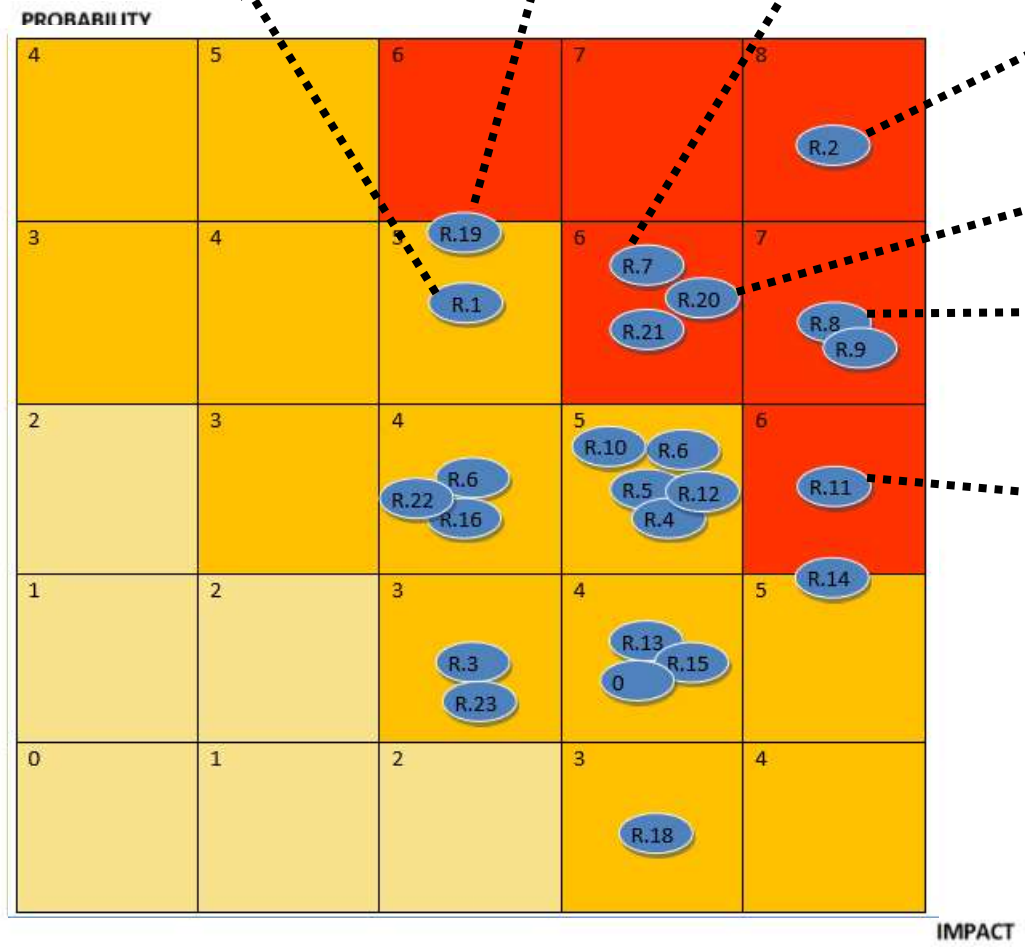
معماری مرجع رایانش ابری: ISO/IEC 17789: 2014



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

کار عملی

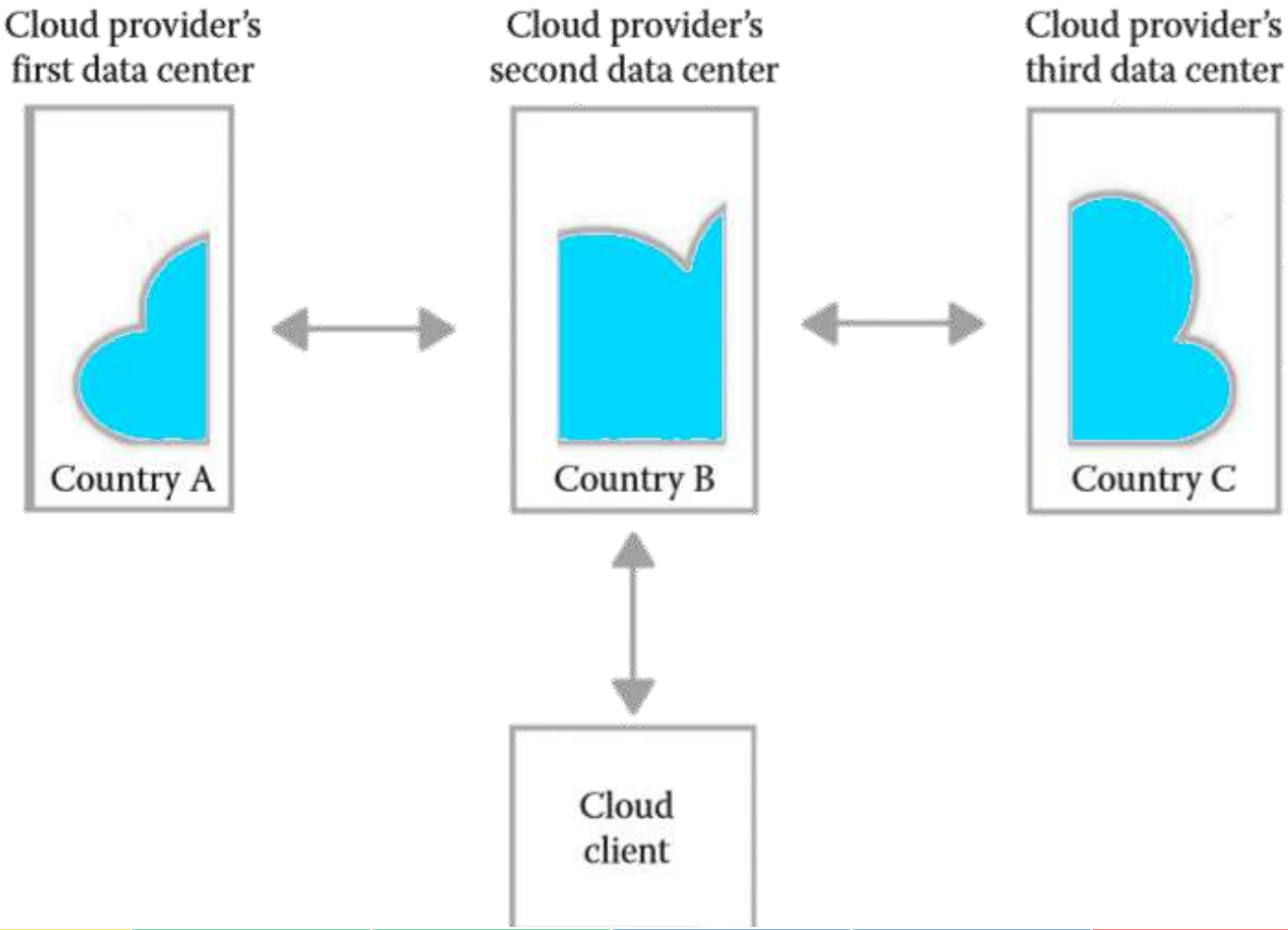
- تحلیل موردی مخاطرات خدمت **پیغام رسانی**
  - قفل شدن در فروشنده (Vendor Lock-in)
  - از دست دادن کنترل (Loss of Governance)
  - شکست زنجیره تامین (Supply chain failure)
  - شکست جداسازی (Isolation Failure)
  - کاربر داخلی بدخواه (Malicious Insider)
  - حمله منع خدمت (Denial of Service)
  - حذف داده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

مخاطره قفل شدن در فروشنده (Lock-in)

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

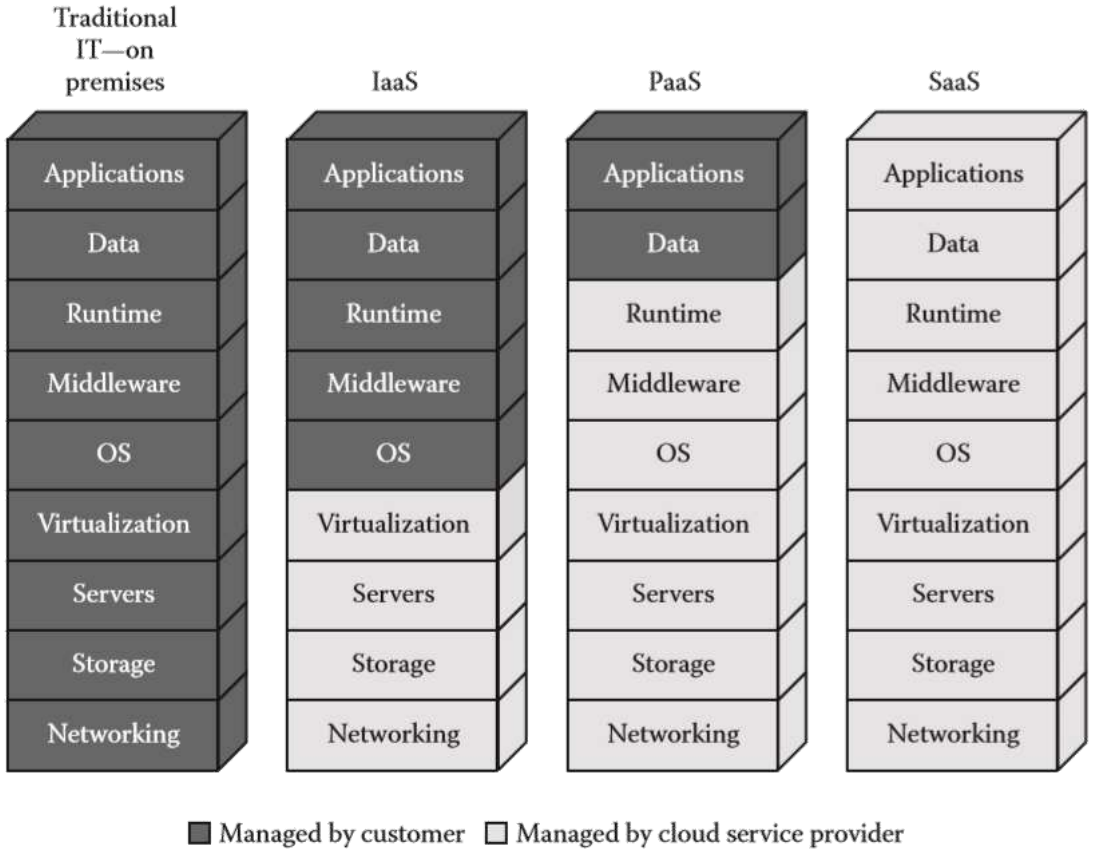
- مثالی از مواردی که ریسک Lock-in پایین است:
  - جابجایی خدمت در خدمات میزبانی / ترابرد بین اپراتورها
- مثالی از مواردی که ریسک Lock-in بالا است:
  - نرم افزارهای پیغام رسان / خدمت پست الکترونیکی / خدمت های سفارشی مدیریت محتوا

مخاطره از دست دادن کنترل (Loss of Governance)



مخاطره از دست دادن کنترل (Loss of Governance)

- 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)

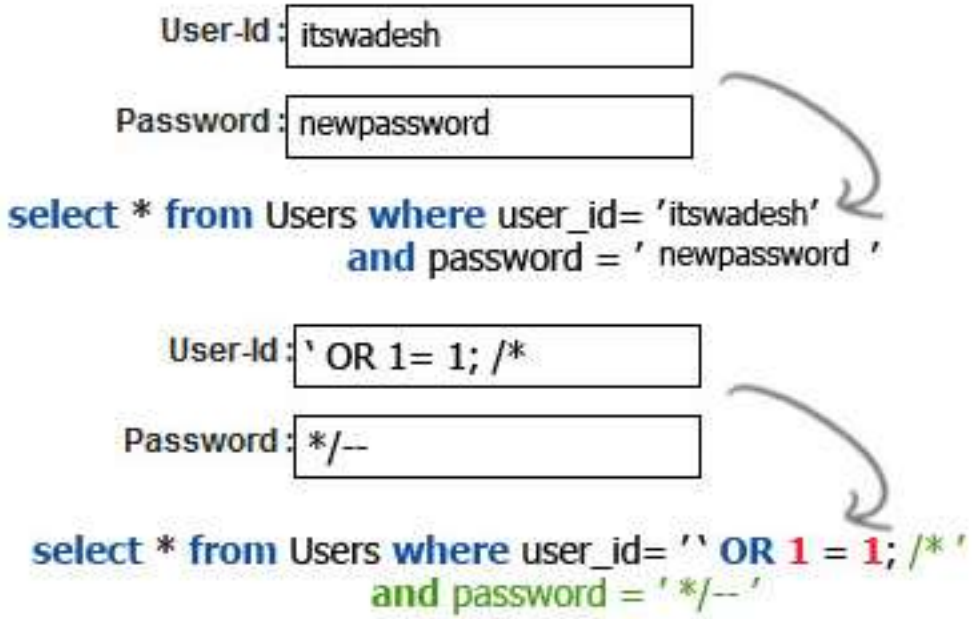
- زمانی پیش می آید که بخشی از فرآیند یک زنجیره تامین بصورت ابری انجام شود و در صورت نقص در ارایه خدمت / نقض محرمانگی و ... ، زنجیره به خطر بیفتد.

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

مخاطره شکست جداسازی (Isolation Failure)

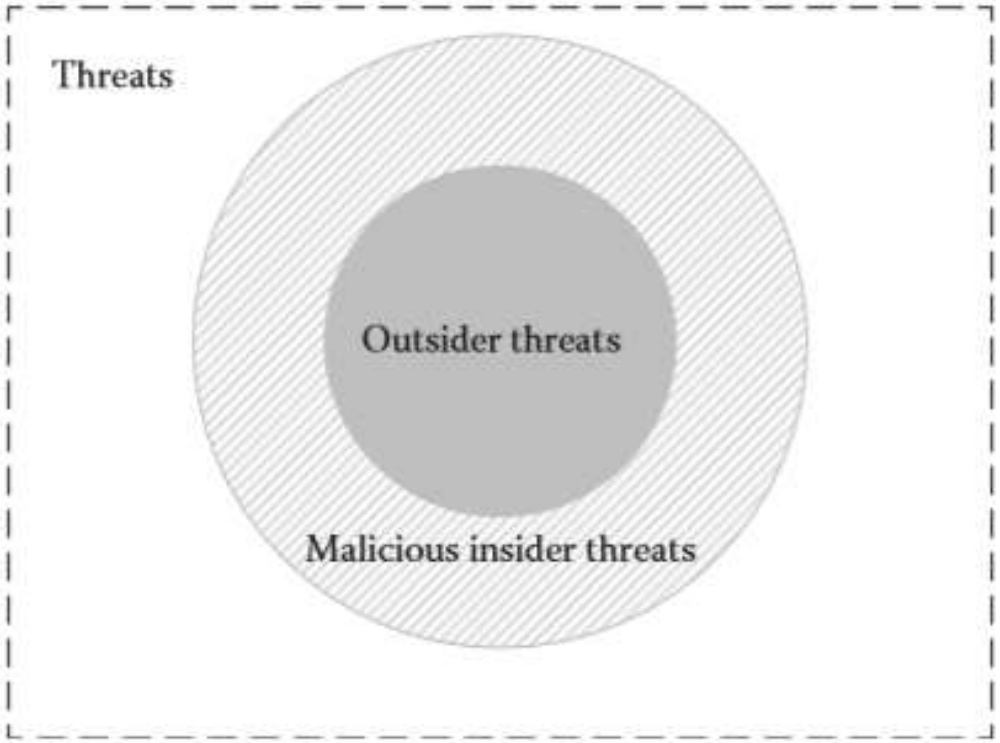
- زمانی اتفاق می افتد که یک مستاجر به منابع / داده مستاجر دیگر دسترسی پیدا کند. (در نتیجه پیکربندی های اشتباه یا آسیب پذیری امنیتی)

- مثال:
  - SQL Injection
  - Spamming
  - Filtering



مخاطره کاربر داخلی بدخواه (Malicious Insider)

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



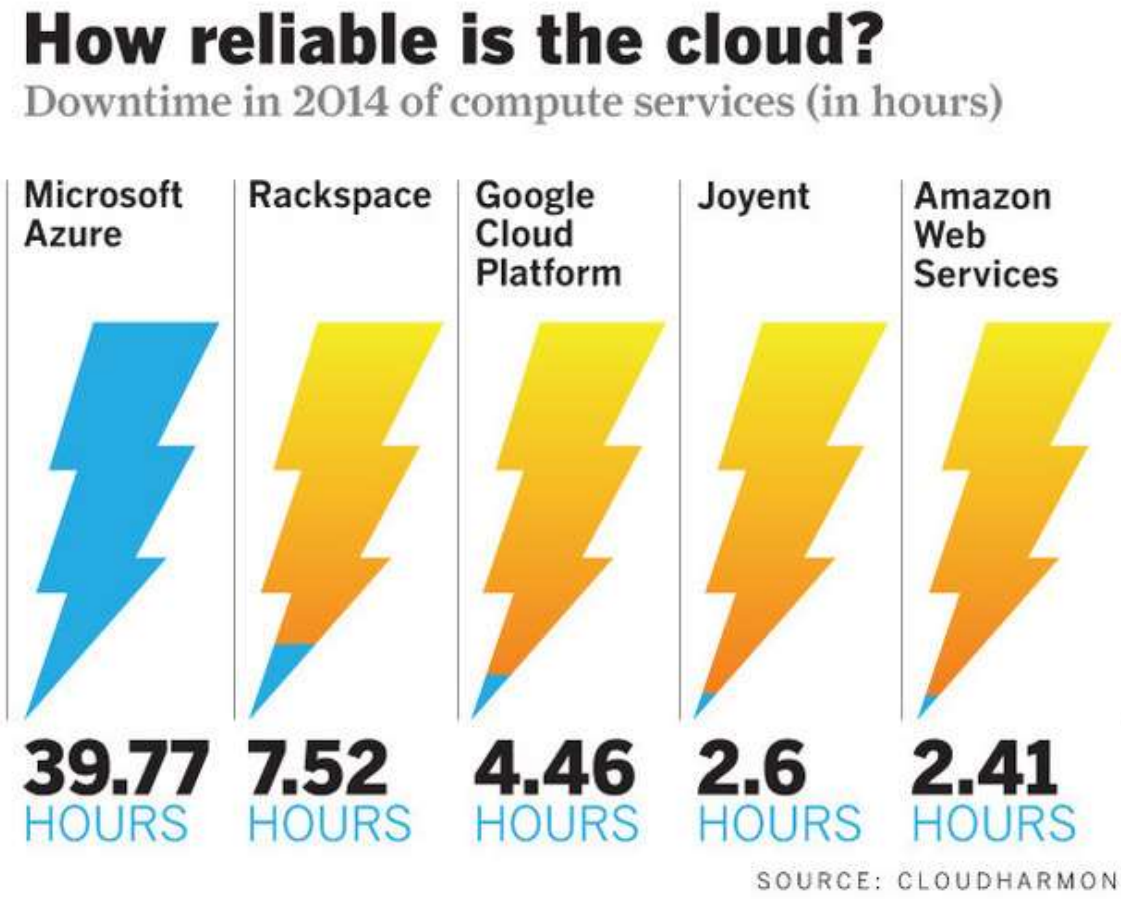
- مثال:
  - کپی اطلاعات
  - تغییر اطلاعات
  - حذف اطلاعات
  - افشای کلمه عبور

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

- 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)

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

مخاطره حملات منع خدمت (DOS)



	Total downtime (HH:MM:SS)		
Availability	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

مخاطره حملات منع خدمت (DOS)

- زمانی اتفاق می افتد که سامانه اشباع شود. (نتواند پاسخگو باشد)
- مثال:
  - بوق اشغال برای دریافت فکس ابری
  - قطع شدن خدمت بخاطر ترافیک بالا

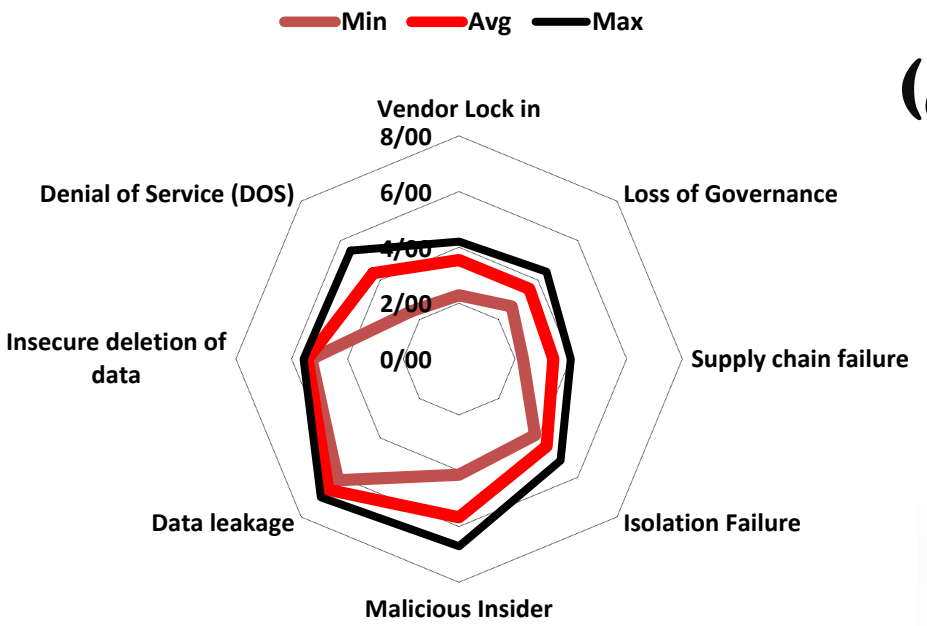
مخاطره از دست رفتن کلیدهای رمزنگاشتی (Loss of Cryptographic Keys)

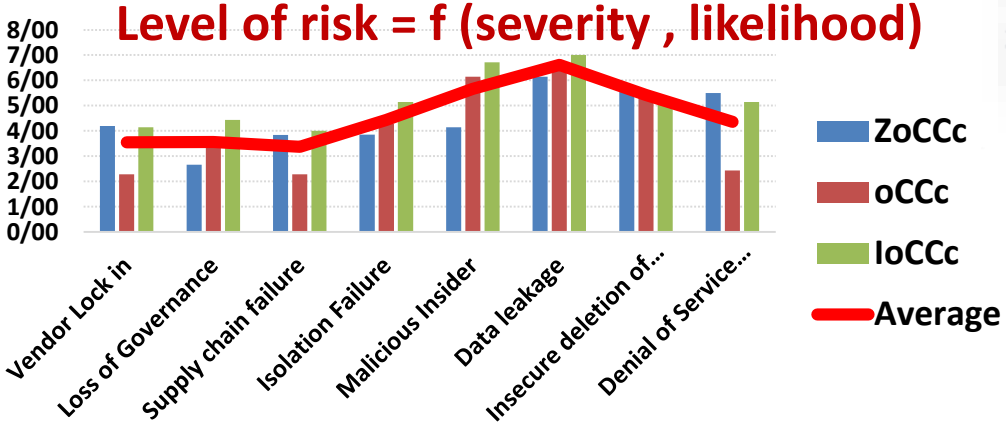
- زمانی اتفاق می افتد که کاربر کلید دسترسی به خدمت را گم کند یا کلید افشا شود که باعث از دست رفتن خدمت یا داده می شود و صدمات مالی در بر دارد.

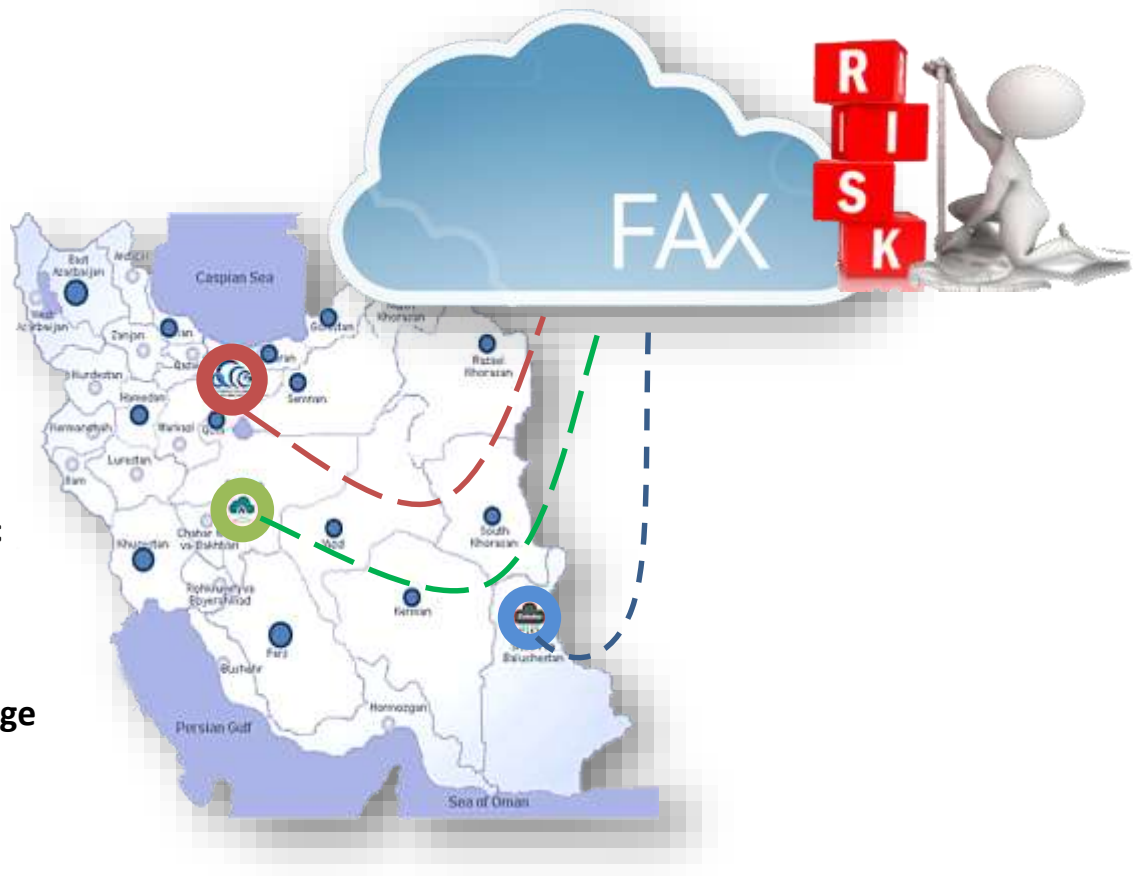
- مثال:
  - کلید های SSL
  - کلیدهای رمزنگاشتی فایل
  - کلیدهای دسترسی به ماشین
  - فراموشی رمز عبور

مثالی از تحلیل مخاطرات در سرویس های ابری

(بررسی موردی فکس ابری در سه جامعه کاربری)



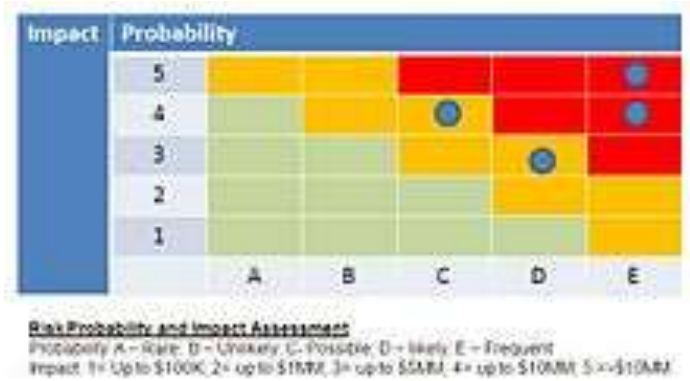




مدیریت مخاطرات حریم خصوصی

PII : Personally Identifiable Information

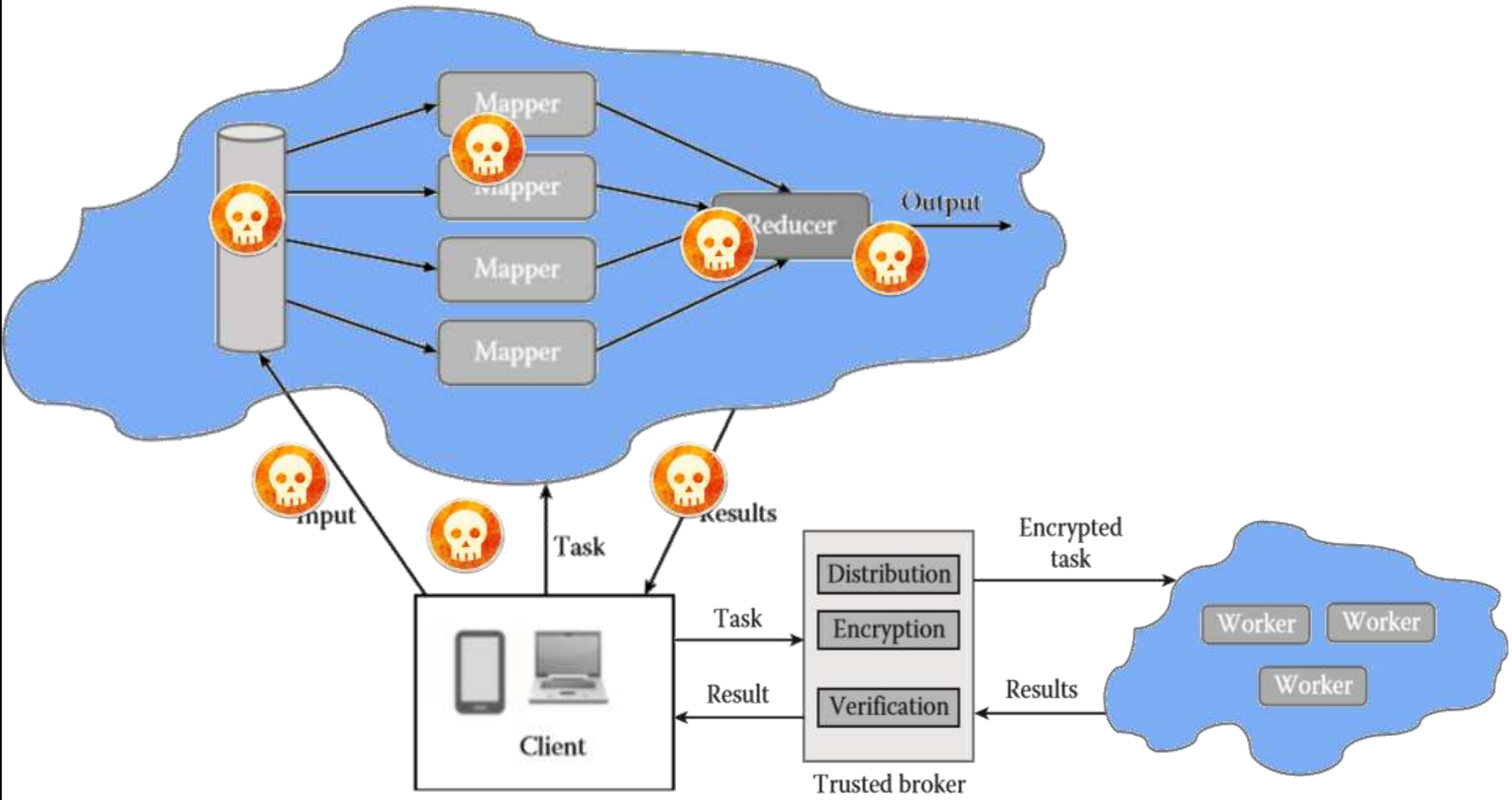
PIA: Privacy Impact Assessment (Tools)



جمع بندی

بده بستان کارآیی و امنیت
نمایش نهایی!

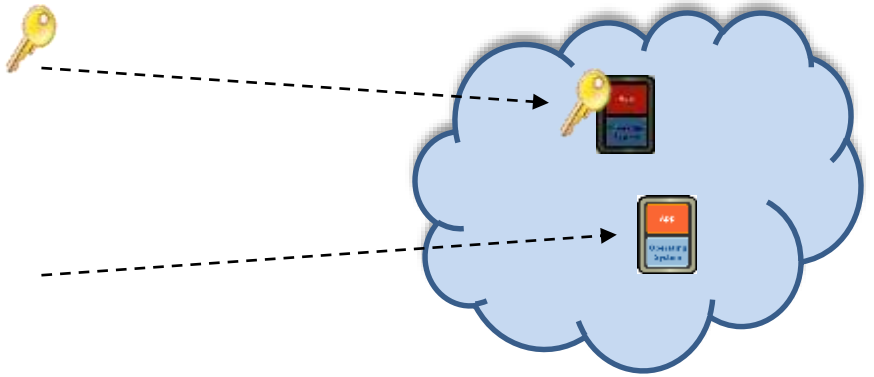
بده بستان کارآیی و امنیت



بده بستان کارآیی و امنیت

پرسمان بر روی داده های رمز شده

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



پرسمان بر روی داده های اصلی (غیررمز)

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

نمایش

با تشکر از توجه شما