امنیت شبکه

جلسه پنجم: کنترل دسترسی شبکه و امنیت محاسبات ابری

تهیه و تنظیم: دکتر آرش حبیبی لشکری

منبع: کتاب اصول و مبانی امنیت شبکه (استانداردها و کاربردها)

اولین نسخه: دی 1393
بروزرسانی: دی 1393

فهرست:

- کنترل دسترسی به شبکه
- پروتکلهای احراز هویت
- محاسبات ابری
- مهماری مرجع محاسبات ابری
- مهمترین تهدیدهای محاسبات ابری

کنترل دسترسی به شبکه

در اصل NAC کاربرانی را که وارد شبکه می‌شوند، اعتبار سنجی نموده و تعیین می‌نماید که به چه داده‌هایی می‌توانند دسترسی پیدا کنند و چه اقداماتی را نیز می‌توانند انجام دهند.

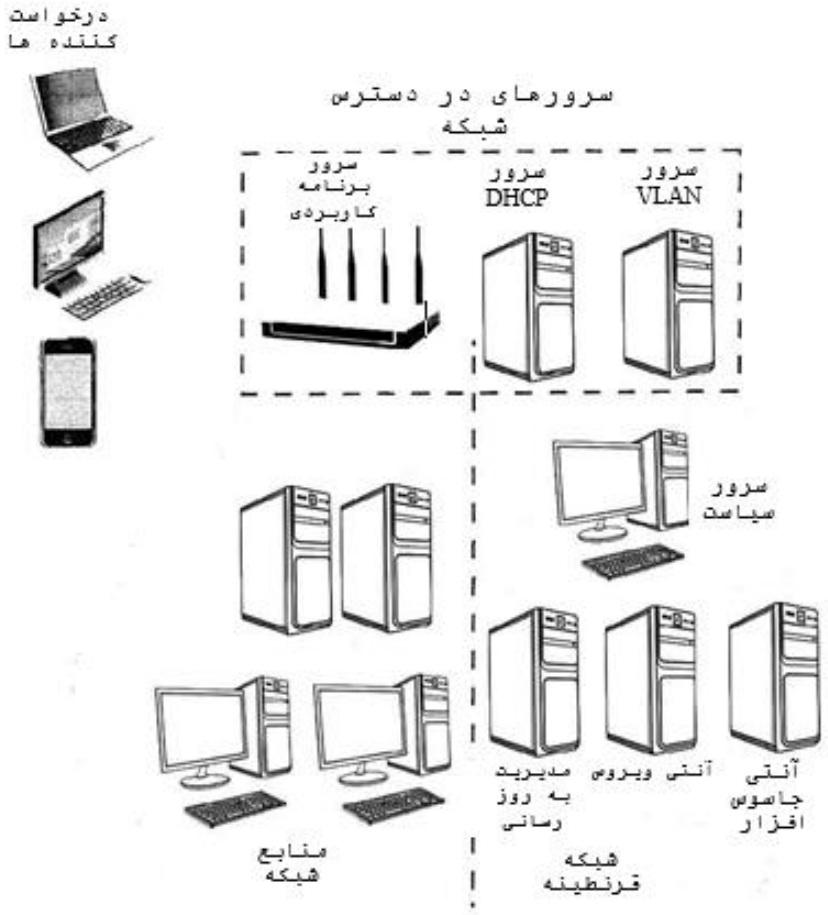
عناصر سیستم کنترل دسترسی به شبکه:

* درخواست کننده دسترسی (AR): در اصل AR گره‌ای است که برای دسترسی به شبکه تلاش می‌کند و ممکن است هرگونه تجهیزی که توسط سیستم NAC مدیریت شود مانند ایستگاه‌های کاری، سرویس‌دهنده-ها، پرینترها، دوربین‌ها و سایر دستگاه‌های فعال شده براساس IP باشد. البته عموما از ARها به عنوان درخواست‌کننده یا مشتری نیز یاد می‌شود.

* سرویس‌دهنده سیاست: بر اساس وضعیت AR و سیاست تعریف شده سازمانی، سرویس‌دهنده سیاست تعیین می‌کند چه دسترسی‌هایی باید به کاربران اعطا شود. سرویس‌دهنده‌های سیاست اغلب به سیستم‌های بخش مدیریت، از جمله آنتی ویروس، مدیریت به روز رسانی و یا یک پوشه کاربری برای کمک به تعیین وضعیت میزبان متکی هستند.

* سرویس‌دهنده دسترسی شبکه (NAS): در اصلNAS بعنوان یک نقطه برای کنترل دسترسی کاربران مکان‌های دور دست به شبکه داخلی شرکت عمل می‌نماید.

مفهوم کنترل دسترسی شبکه



هدف: جلوگیری از دسترسی کاربران آسیب پذیر و ناموافق به شبکه

سوال: چرا احراز هویت (802.1X) کافی نیست؟

متدهای اجرای دسترسی به شبکه

* پروتکل IEEE802.1X: یک پروتکل لایه اتصال است که احراز هویت را پیش از اینکه یک گذرگاه به یک آدرس IP اختصاص یابد، اعمال می‌نماید. این استاندارد از پروتکل احراز هویت گسترش یافته برای پردازش احراز هویت استفاده می‌نماید.

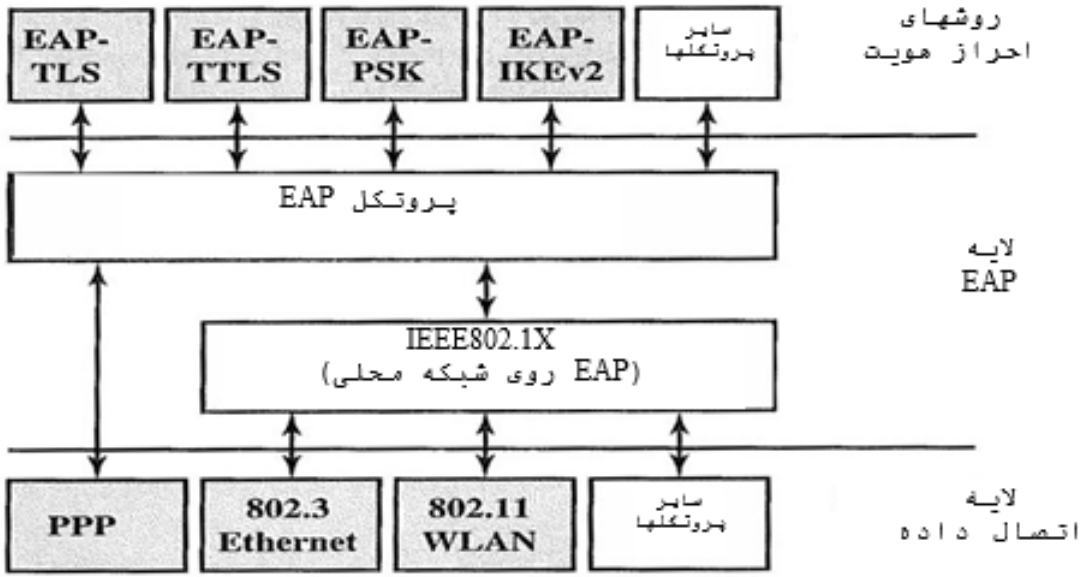
* شبکه‌های محلی مجازی (VLANs): در این خطمشی، شبکه‌های بزرگ سازمانی، با عنوان اتصال مجموعه‌ای از شبکه‌های محلی درنظر گرفته می‌شوند که بطور منطقی به چندین شبکه محلی مجازی تقسیم شده‌اند.

* دیوارآتش: دیوارآتش یک نمونه NAC را از طریق اجازه‌دادن یا ردکردن ترافیک‌های رد و بدل شده بین شرکت میزبان و کاربر خارجی ایجاد می‌کند.

* مدیریت DHCP: پروتکل پیکربندی پویای میزبان یا همان DHCP یک پروتکل اینترنتی است که امکان تخصیص پویای آدرس‌های IP را به میزبانهای یک شبکه می دهند. یک سرویس‌دهنده DHCP درخواستهای رسیده به DHCP را ردگیری نموده و به میزبانها آدرس IP پویا اختصاص می‌دهد.

پروتکل احراز هویت توسعه پذیر EAP

در اصل EAP یک سرویس عمومی برای تبادل اطلاعات احرازهویت مابین مشتری و سرویس‌دهنده احراز هویت فراهم می نماید. از آنجایی که این پروتکل از روش‌های تایید هویت چندگانه که می بایست روی ماشین مشتری و سرویس دهنده نصب شود، پشتیبانی می‌نماید لذا به آن توسعه پذیر می گویند.



ساختار عمومی پیامها در EAP

پیامهای EAP ممکن است شامل فیلدهای زیر باشند:

- **کد:** نوع پیام EAP را مشخص می‌نماید.

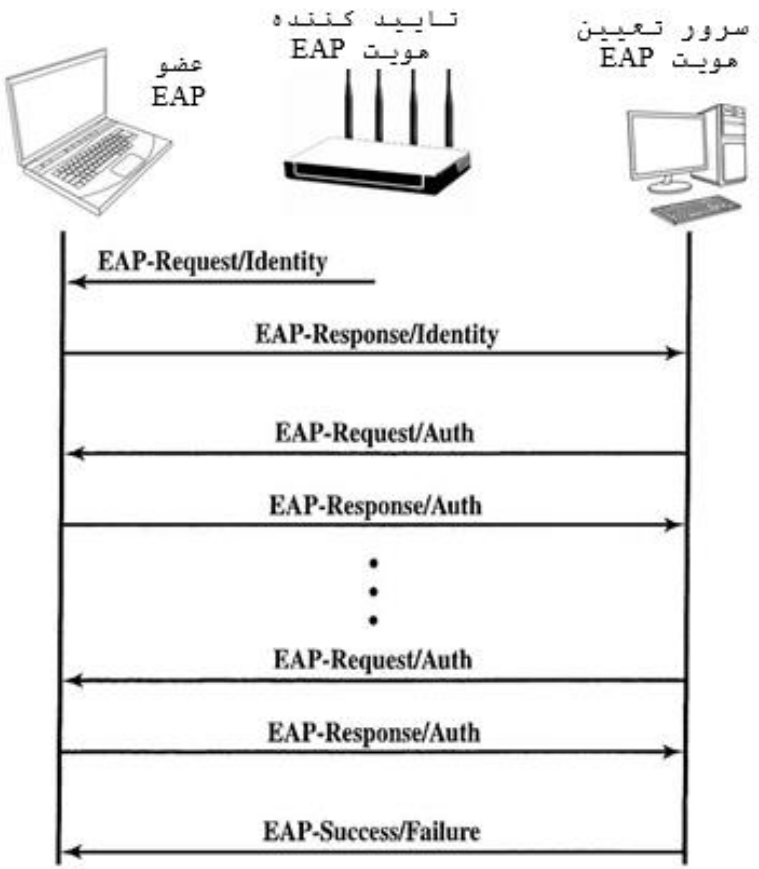
کدها بصورت : درخواست (1)- پاسخ (2) – موفقیت (3) – شکست (4) هستند.

- **شناسه:** برای تطابق پاسخ با درخواست مورد استفاده قرار می‌گیرد.

- **طول:** طول پیام EAP را در کلمات هشت بیتی، شامل کد، شناسه، طول، و فیلد داده نمایش می‌دهد.

- **داده:** شامل اطلاعات مربوط به احراز هویت است. به طور معمول، فیلد "داده" شامل زیر فیلد "نوع"، که نوع داده حمل شده را نشان می‌دهد، و یک فیلد" نوع داده" است.

مثال برای پروتکل EAP

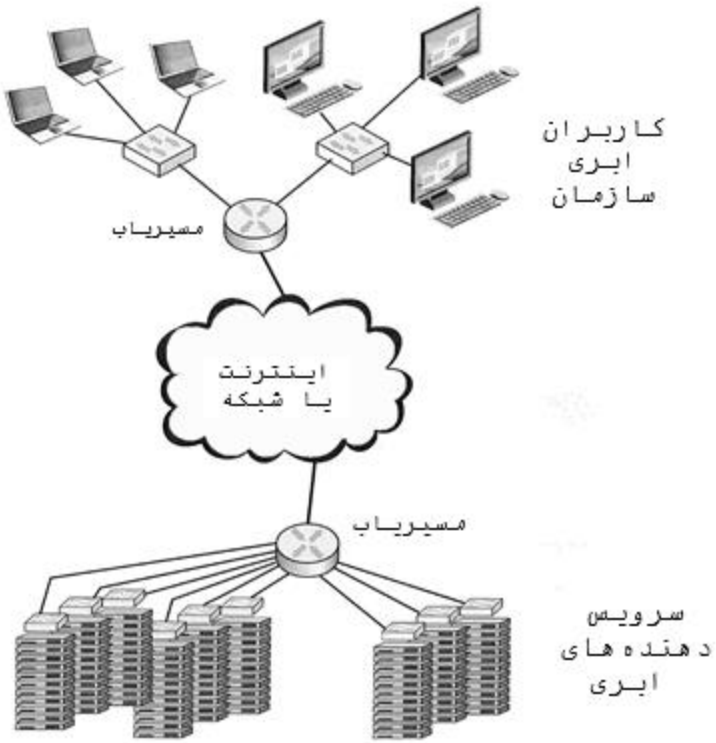


یک پروتکل که برای این منظور مورد استفاده قرار گرفته است پروتکل IEEE 802.1X است که در بخش بعدی مورد استفاده قرار خواهد گرفت. اولین جفت پیام درخواست و پاسخ EAP همان نوع هویت است، که در آن تأیید کننده اعتبار هویت عضو نظیر را درخواست نموده و عضو نظیر هویت مطالبه شده را در پاسخ پیام برمی‌گرداند. این پاسخ از طریق تأییدکننده اعتبار برای احراز هویت به سرویس‌دهنده منتقل می‌شود. پیامهای EAP بعدی بین عضو نظیر و سرویس‌دهنده احراز هویت رد و بدل خواهند شد.

محاسبات ابری

محاسبات ابری

مدلي است براي ايجاد دسترسي از همه-جا، به صورتي مناسب از طريق شبكه به يك مجموعه‌اي از منابع پردازشي قابل پيكربندي (مانند شبكه‌ها، سرويس‌دهنده-ها، منابع ذخيره‌سازي، برنامه‌هاي كاربردي و ساير خدمات) كه بتواند به سرعت تدارك ديده شده و با حداقل فعاليت‌هاي مديريتي يا تعاملات با ارائه-كننده سرويس‌ها، در اختيار كاربران قرار گيرد. اين مدل ابری ميزان دسترس‌پذيري را بهبود داده و از پنج خصوصيت اساسی، سه مدل خدماتي و چهار مدل براي گسترش مدلهای ابری تشكيل شده است.



خصوصيات اصلی محاسبات ابری

* **دسترسي وسيع به شبكه:** قابليت‌ها از طريق شبكه و با استفاده از سازوكارهاي استانداردي مورد دسترسي قرار مي‌گيرند كه نرخ استفاده آن‌ها از طرف مشتري‌هايي با زيرساختهای غير متجانس (مانند، تلفن‌هاي همراه، رايانه‌هاي قابل حمل، و PDAها) افزايش يافته و بخوبی ساير خدمات نرم-افزاری سنتي يا مبتني بر ابرها خواهد شد.

* **قابليت واكنشی سريع:** محاسبات ابري اين قابليت را در اختيار كاربر قرار مي‌دهند كه بتواند منابعي را كه در اختيار دارد بر اساس نيازمندي‌هاي خدماتي خاص كاربر افزايش يا كاهش دهد.

* **سرويس اندازه‌گيري شده:** سيستم‌هاي ابري به صورت خودكار، ميزان استفاده از منابع را موردكنترل و بهينه‌سازي قرار مي‌دهند.

* **سرويس دهی به خود در هنگام تقاضا:** يك مشتري مي‌تواند به صورت يك‌طرفه و خودكار و بدون اين‌كه نياز به برقراری تعامل با ارائه‌دهندگان خدمات داشته باشد، قابليت‌هاي محاسباتي خاصی را در هر زماني كه مورد نياز باشند، مثل زمان سرويس‌دهنده و فضاي ذخيره‌سازي اطلاعات قابل دسترسي از طريق شبكه ،براي خود تدارك ببيند.

* **به اشتراك گذاري منابع:** منابع محاسباتي ارائه‌كننده در يك استخری از منابع قرار داده مي‌شوند تا بتوانند توسط مشتريان مورد استفاده اشتراكي قرار گيرند.

انواع مدلهای سرویس محاسبات ابری

- **نرم افزار بعنوان سرويس :** قابليتي كه به يك مشتري ارائه مي‌شود در اصل استفاده از برنامه‌هاي كاربردي ارائه‌دهنده‌ي خدمات است كه بر روي يك زير ساخت ابري در حال اجرا مي‌باشند.

- **پایگاه نرم افزاری به عنوان سرویس:** قابلیت ارائه شده به مصرف‌کننده برای استقرار بر روی زیرساخت‌های محاسبات ابری ایجاد شده، توسط مشتری و یا دست یافتن به برنامه‌های کاربردی ایجاد شده با استفاده از زبانهای برنامه‌نویسی و ابزارهای پشتیبانی شده توسط ارائه دهنده، به کار می‌رود.

- **زیرساخت به عنوان یک سرویس:** قابلیت ارائه شده به مصرف‌کننده برای تدارک وسایل لازم برای پردازش، ذخیره‌سازی، شبکه‌ها، و دیگر منابع محاسبات اساسی می‌باشد که در آن مصرف کننده قادر به استقرار و اجرای نرم‌افزارهای دلخواهی است که می‌تواند شامل سیستم‌های عامل و برنامه‌های کاربردی باشند.

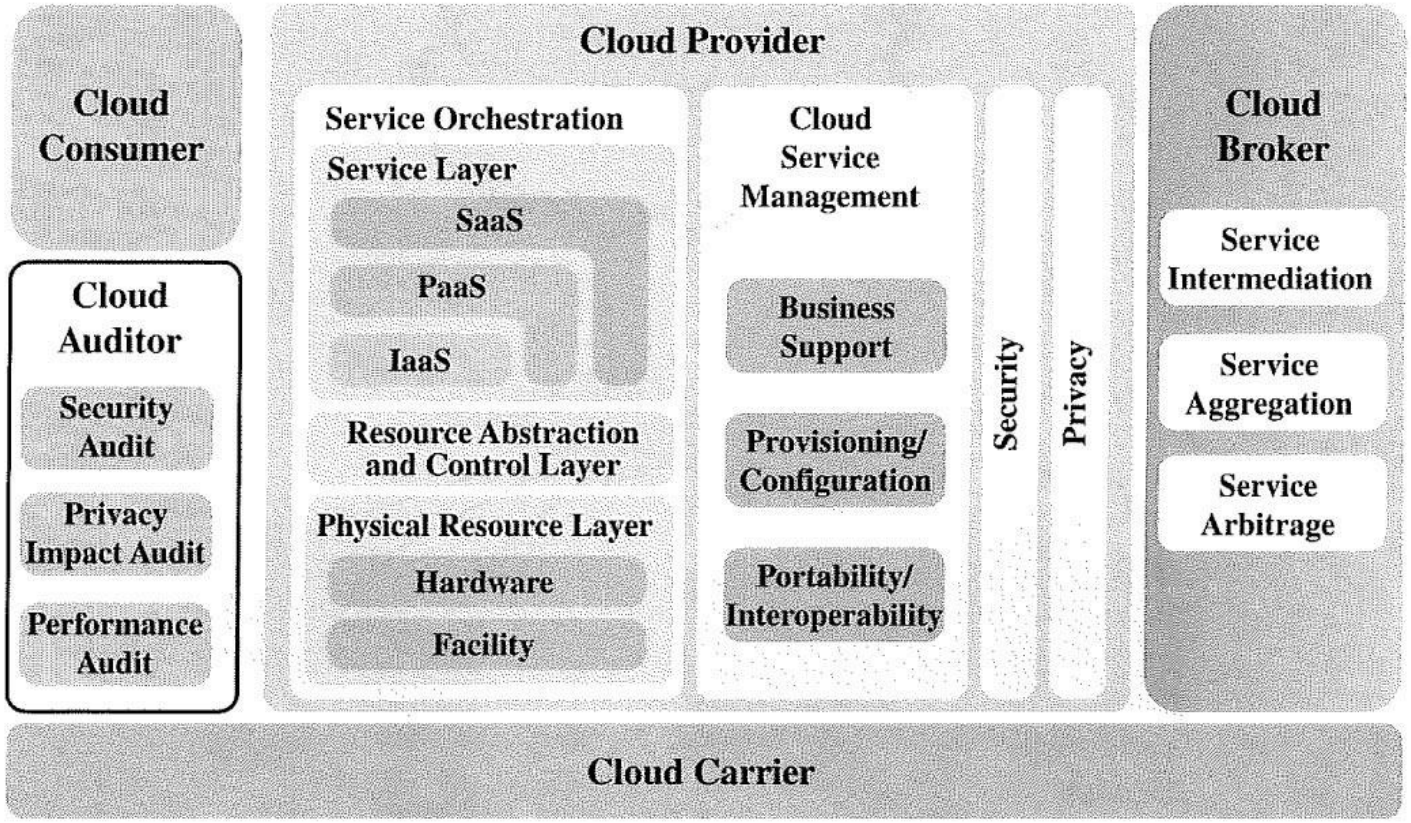
معماری مرجع محاسبات ابری

معماری مرجع محاسبات ابری NIST روی نیازمندیهای اینکه "چه" سرویسهای ابری ارائه می‌شوند، تمرکز دارد نه روی اینکه "چگونه" می‌توان راه‌حلی را طراحی و پیاده‌سازی نمود. معماری مرجع قصد دارد تا درک عملیات پیچیده داخل محاسبات ابری را آسان سازد. برخلاف تصور این معماری سعی در نمایش معماری سیستمی یک سیستم خاص محاسبات ابری را نداشته و در عوض ابزاری است برای شرح، بحث و پیاده‌سازی یک معماری خاص - سیستمی با استفاده از قالب عمومی مرجع.

در اصل NISTمعماری مرجع را با در نظر گرفتن اهداف زیر توسعه داده است:

- برای مصور نمودن و درک سرویسهای مختلف ابری در زمینه یک مدل مفهومی محاسبات ابری کلی
- مهیا نمودن یک مرجع فنی برای مشتریان جهت درک، بحث، دسته‌بندی و مقایسه سرویسهای ابری
- آسان نمودن تجزیه و تحلیل استانداردهای نامزد شده برای امنیت، قابلیت همکاری، و قابلیت حمل و پیاده سازی مرجع

معماری مرجع محاسبات ابری



اعضای اصلی در معماری مرجع

- **مصرف کننده ابر**: یک شخص یا سازمانی که یک ارتباط تجاری را با ارائه دهندگان خدمات ابری ایجاد نموده و از سرویسهای آنها استفاده می‌نماید.

- **ارائه‌دهنده ابر:** یک شخص، سازمان، یا نهاد مسئول برای دسترس پذیر نمودن خدمات برای واحدهای علاقه‌مند.

- **بازرس ابر:** تیمی که می‌تواند ارزیابی مستقلی روی خدمات ابر، عملیات سیستم اطلاعات، عملکرد و امنیت پیاده سازی شده در ابر انجام دهد.

- **کارگزار ابر:** یک موجودیتی که استفاده، کارایی، و ارائه خدمات محاسبات ابری، و روابط بین ارائه دهندگان خدمات ابری و مصرف‌کنندگان خدمات ابری را مدیریت می‌نماید.

- **حامل ابر**: واسطه‌ای که اتصال و انتقال خدمات ابری را بین فراهم‌کننده خدمات ابری و مصرف کننده خدمات ابری میسر می‌سازد.

مهمترین تهدیدات امنیتی خاص محاسبات ابری

- **سوء استفاده و استفاده نابهنجار از محاسبات ابری:** برای بسیاری از CPها ثبت نام و شروع به استفاده از خدمات ابری نسبتا آسان است، حتی برخی از آنان دوره‌های آموزشی مجانی محدودی را نیز برگزار می‌نمایند. این امر این امکان را به مهاجمین می‌دهد تا وارد ابر محاسباتی شده و حملات مختلفی مانند هرزنامه، حمله کد مخرب و حمله محرومیت از خدمات را انجام - دهند.
- **رابطهای ناامن و APIها:** در اصل CPها مجموعه‌ای از رابطهای نرم‌افزاری یا APIها را نمایش می‌دهند که مشتریان برای مدیریت و تعامل با خدمات ابری از آنها استفاده می‌کنند. امنیت و در دسترس بودن خدمات عمومی ابر به امنیت APIهای پایه بستگی دارد.
- **بداندیشان داخلی:** طبق نمونه محاسبات ابری، سازمان ازکنترل مستقیم بر بسیاری از جنبه‌های امنیتی صرفنظر نموده و در نتیجه انجام این کار، سطح بی‌سابقه‌ای از اعتماد را به CP اعطا خواهد نمود. یکی از نگرانی‌های بزرگ و مهم در هر سازمان کارمندان داخلی بداندیش هستند. (مدیران سیستم CP و ارائه دهندگان خدمات امنیتی)
- **مسائل مربوط به فن‌آوری به اشتراک گذاشته شده:** فروشندگان IaaS خدمات خود را از روش‌های مقیاس‌پذیر مربوط به اشتراک‌گذاری زیرساخت‌ها ارائه می‌دهند. اغلب، اجزای اساسی که این زیرساخت‌ها را تشکیل می‌دهند (مانند حافظه سریع CPU، GPUها، و غیره) برای ارائه خواص جداسازی قوی برای یک معماری چند کاربره طراحی نشده‌اند. (استفاده از ماشین‌های مجازی ایزوله شده برای مشتریان مجزا).
- **خطرهای ناشناخته:** در استفاده از زیرساخت‌های ابر، مشتری تنها در مسائلی که ممکن است برامنیت تاثیر بگذارد کنترل را به CP تخصیص می‌دهد. بنابراین مشتری باید به وضوح نقش‌ها و مسئولیت‌هایی که مربوط به مدیریت ریسک هستند را بداند. برای مثال، کارکنان ممکن است برنامه‌ها و منابع داده در CP را بدون رعایت سیاست‌های معمولی برای حفظ حریم خصوصی، امنیت و نظارت توسعه دهند.

برای هر نوع تهدید راهکارهای مناسبی را ارائه نمایید؟

محافظت داده ها در ابر (یک مثال امنیتی)

راههای زیادی برای تخریب داده‌ها وجود دارد. حذف و یا تغییر سوابق بدون گرفتن نسخه پشتیبان از محتوای اصلی یکی نمونه‌های بارز تخرب داده‌هاست. لغو پیوند یک رکورد از یک فایل ممکن است آنرا غیر قابل اصلاح نماید، همانطور که می‌تواند بر روی یک رسانه غیر قابل اعتماد ذخیره گردد. از دست دادن یک کلید رمزنگاری ممکن است به تخریب موثرتری منجر شود. ودر نهایت، طرفین غیر مجاز باید از دسترسی به اطلاعات حساس منع شوند.

در اینجا چهار موجودی درگیر هستند:

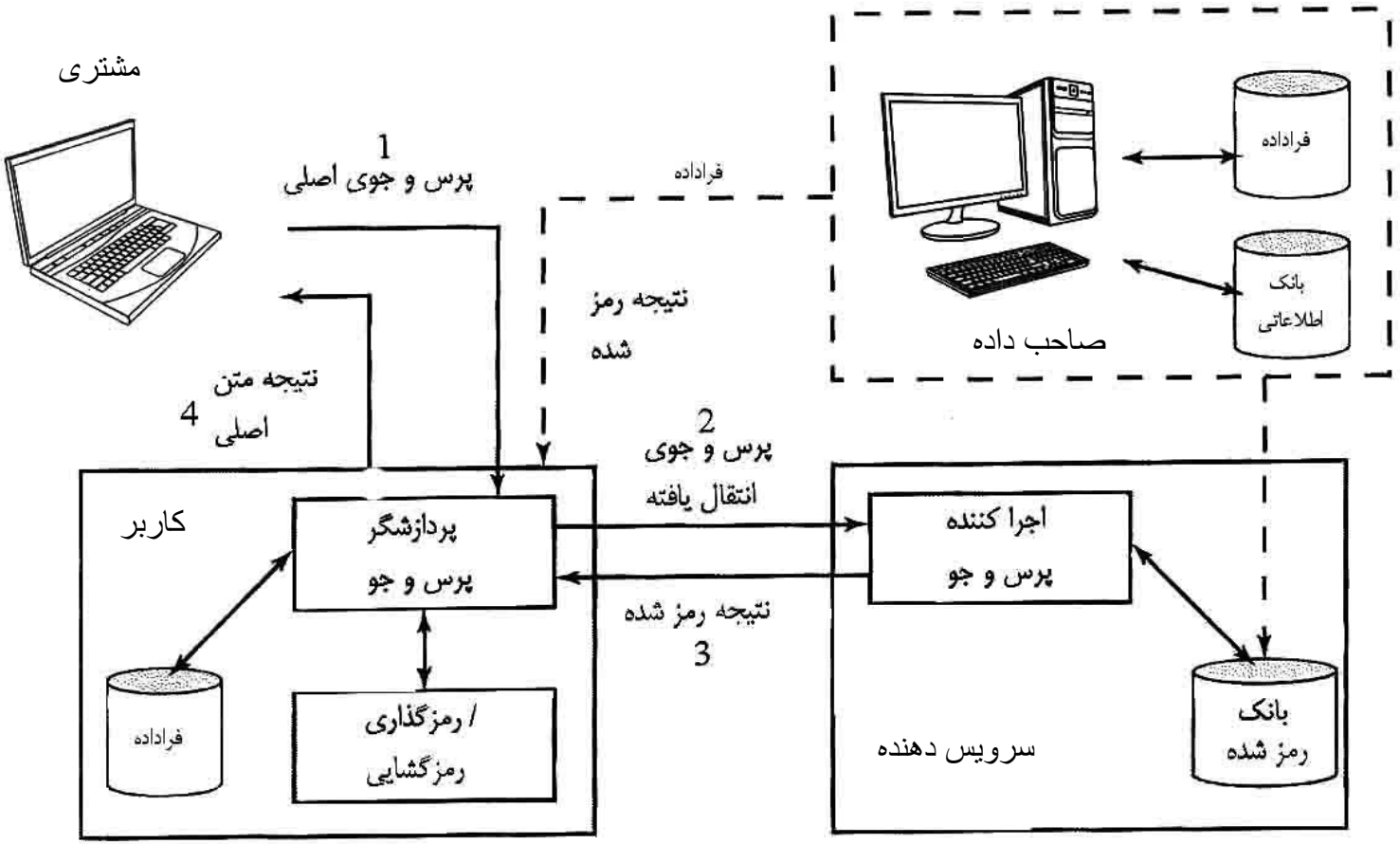
- **صاحب داده‌ها:** سازمانی است که اطلاعات را برای انتشار کنترل شده، چه در درون سازمان و چه برای کاربران خارجی در دسترس قرار می‌دهد.

- **کاربر:** موجودیت انسانی که تقاضاها (پرسشها) را به سیستم ارائه می‌دهد.کاربر می‌تواند یکی از کارکنان سازمان باشد که از طریق سرویس‌دهنده به پایگاه داده‌ها دسترسی دارد و یا یک کاربر خارجی باشد که سازمان پس از احراز هویت، به او حق دسترسی اعطا کرده است.

- **مشتری**: کامپیوتر یا نرم‌افزاری که پرس و جوی کاربر را به یک پرس و جو در داده‌های رمزگذاری شده ذخیره شده بر روی سرویس‌دهنده تبدیل می‌کند.

- **سرویس‌دهنده**: سازمانی که داده‌های رمزگذاری شده را از مالک داده‌ها دریافت نموده و آنها را برای توزیع به مشتریان در دسترس می‌سازد. سرویس‌دهنده می‌تواند در واقع متعلق به مالک داده، اما به طور معمول، یک مرکز متعلق و نگهداری شونده توسط ارائه دهنده‌های خارجی باشد. در این بحث، منظور از سرویس‌دهنده همان سرویس دهنده ابر است.

مدل رمزگذاری برای یک پایگاه داده - ابری



امنیت ابر به عنوان یک سرویس

اصطلاح امنیت به عنوان سرویس یا Secaas، بطور کلی بسته‌ای از سرویس‌های امنیتی ارائه شده توسط یک ارائه‌دهنده سرویس است که مقدار زیادی از مسئولیت‌های امنیتی را از سازمانها به ارائه-دهندگان سرویس امنیتی انتقال می‌دهد. از میان سرویس‌ها آنتی ویروس، ضد بدافزار یا جاسوس‌افزار، کشف حمله، و مدیریت حوادث امنیتی آنهایی هستند که معمولا ارائه شده‌اند.

دسته‌بندیهای سرویس SecaaS:

- موجودیت و مدیریت دسترسی
- پیشگیری از گم‌شدن داده‌ها
- امنیت WEB
- امنیت پست- الکترونیکی
- بازرسی امنیت
- مدیریت نفوذ
- اطلاعات امنیتی و مدیریت رویداد
- رمزگذاری
- تداوم تجارت و جبران فاجعه
- امنیت شبکه

سوالات مرتبط

1. بطور خلاصه کنترل دسترسی شبکه را تعریف نمایید.
2. پروتکل اعتبار سنجی قابل توسعه چیست؟
3. چهار روش شناسایی EAP را نام برده و شرح دهید.
4. وظیفه IEEE 802.1X چیست؟
5. محاسبات ابری را تعریف نمایید.
6. بطور خلاصه سه مدل سرویس دهی ابری را نام برده و شرح دهید.
7. معماری مرجع محاسبات ابری چیست؟
8. چند تهدید اساسی مخصوص امنیت محاسبات ابری را شرح دهید.

خلاصه: کنترل دسترسی به شبکه، پروتکلهای احراز هویت، محاسبات ابری، معماری مرجع محاسبات ابری، مهمترین تهدیدهای محاسبات ابری

جلسه بعدی:
امنیت لایه انتقال

منبع: کتاب اصول و مبانی امنیت شبکه (استانداردها و کاربردها)

ترجمه: دکتر آرش حبیبی لشکری، مهندس نسرین بدیع، مهندس فرنار توحیدی

هیچ راهی برای به دست آوردن تجربه به جز از
طریق تجربه وجود ندارد.