Security in cloud computing

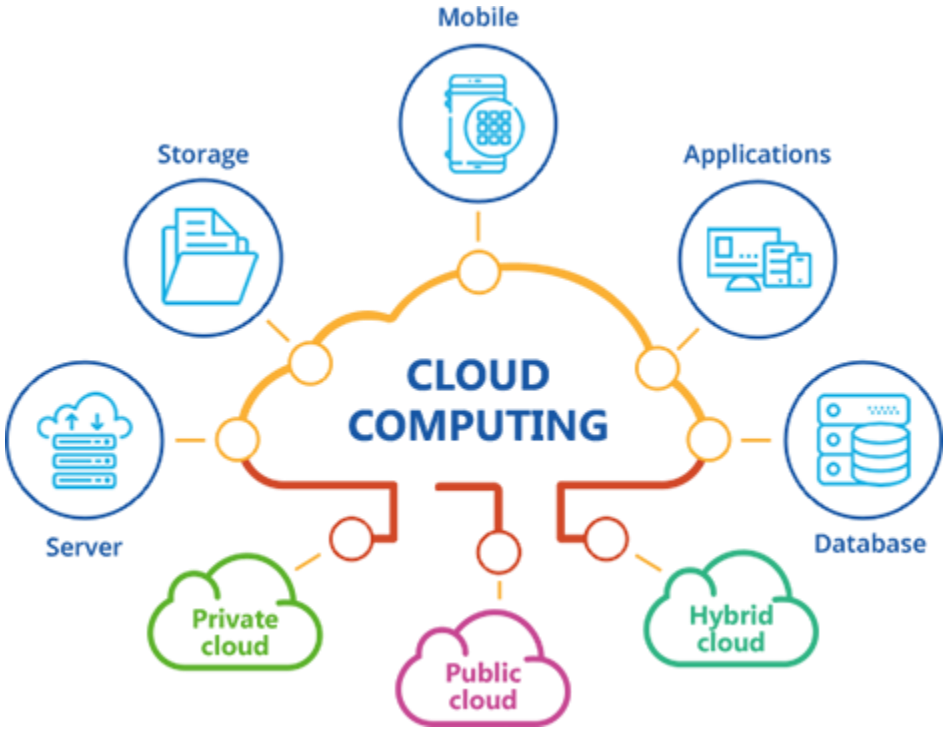
امنیت در رایانش ابری

اتوسا طغیانی – دانشگاه لرستان

بهار ۹۹

مقدمه:

رایانش ابری ، یک مدل مبتنی بر اینترنت است که برای ایجاد دسترسی به دریایی از منابع محاسباتی است.
این منابع می‌توانند: شبکه، سرور، سرویس و یا اپلیکیشن باشند.
محاسبات، به معنای توان پردازشی است که از سوی خدمات ابری ارائه می‌شود و هر چه توان محاسباتی بیشتر باشد به همان نسبت عملکرد بهتر است.



ابر برای اتصال ارزان، مسیریابی و مدیریت در هر زمان و مکانی بسیار کارآمد خواهد بود. داده های ابر با کمک خدمات ارائه‌شده توسط ارائه‌دهندگان خدمات ابری در یک سرور از راه دور ذخیره می‌شوند و قابل‌دسترسی هستند.

تامین امنیت یک نگرانی اساسی است، زیرا داده‌ها از طریق یک کانال (اینترنت) به سرور از راه‌دور منتقل می‌شوند. امنیت داده‌ها درسرور پایگاه داده ابری، منطقه اصلی نگرانی در پذیرش ابر است. برای محافظت از داده ها "رمزگذاری" یکی از روش‌های مهم است.

مقدمه:

طبق گزارشات ۱۰ استارتاپ برتری که در مقیاس جهانی در زمینه رایانش ابری به فعالیت اشتغال دارند، موفق شده‌اند بیش از ۷۳۶ میلیون دلار بودجه از سرمایه‌گذاران خطرپذیر به‌دست اورند.

بزرگان این حوزه آمازون (AWS) ، مایکروسافت (Microsoft Windows Azure) ، گوگل (GCP)، آی بی ام (IBM) و به‌تازگی علی بابا (Alibaba) هستند.

باتوجه به این‌که این فناوری یک فناوری جدید نوظهور است؛ اما رشد خوبی داشته است و در تمام این رشد، امنیت نقش اساسی دارد.

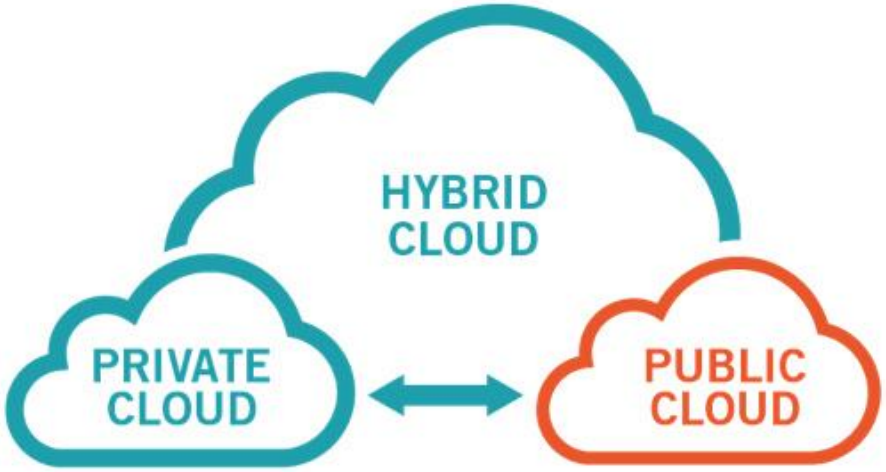
انواع ابر:

- ابر عمومی:

برای عموم مردم یا گروه بزرگی از صنعت قابل دستیابی است و توسط شخص ثالثی که خدمات ابری را می‌فروشد، ارائه می‌شود.

- ابرخصوصی:

تنها مختص یک سازمان یا شرکت خاص بوده که دسترسی کامل و ایمنی به ان دارد و تنها کاربران و مشتریان مشخص می‌توانند در ان فعالیت کرده و از سرویس‌های ان استفاده نمایند.



- ابر ترکیبی :

ترکیبی از ابرخصوصی و ابرعمومی است که با استفاده از تکنولوژی، این ابرها به یکدیگر متصل می‌شوند و امکان به اشتراک گذاشتن داده‌ها و اپلیکیشن‌ها بین آن‌ها فراهم می‌شود؛ این نوع ابر، موجب انعطاف‌پذیری بیشتر کسب‌وکارها می‌شود و امکانات گسترده‌تری را در اختیار آن‌ها قرار می‌دهد.

سرویس دهی در ابر:

IaaS:

درمدل IaaS منابع خام پردازشی در اختیار کاربر قرار میگیرد،که شامل: سرورها، ذخیره‌سازها ، شبکه ها و... است.

نمونه ایی از خدمات فروشنده های این مدل: cloud Amazon، Go Grid، Rackspace Cloud

PaaS:

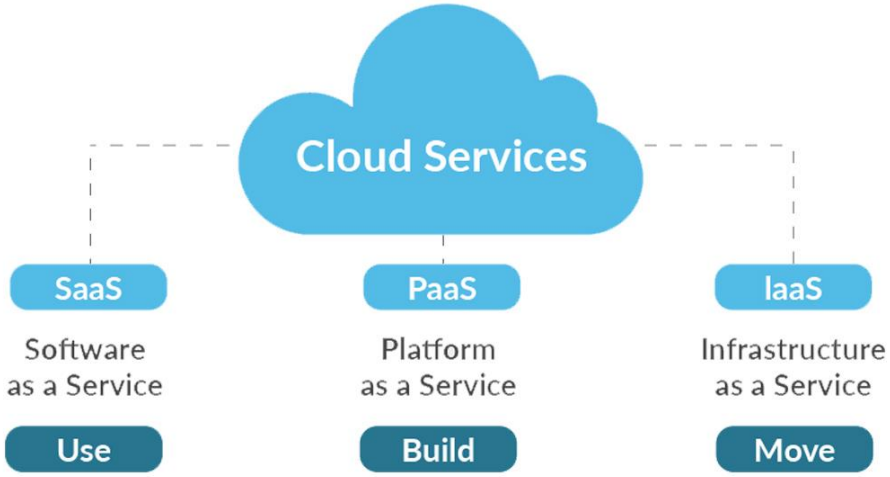
در این مدل پلتفرم در اختیار کاربران قرارمی‌گیرد تا برنامه‌های مورد نیاز خود را روی آن نصب کنند.

نمونه‌ایی از خدمات فروشنده‌های این مدل: Microsoft Windows Azure, Amazon Web Service Elastic Beanstalk

SaaS :

در مدل SaaS کاربران با استفاده از مرورگرهای وب از طریق اینترنت، به نرم افزارهای کاربردی سرویس دسترسی پیدا می‌کنند.

نمونه هایی از خدمات فروشنده های این مدل: Google Docs ,Saleforce.com(CRM), Google Gmail



سرویس دهی در ابر:

IaaS:

مزایا:

مقیاس‌گذاری پویا

مجازی‌سازی دسک‌تاپ

خطرات:

تهدیدات امنیتی ناشی از میزبان

حمله DOS

حملات اتصال به شبکه و اینترنت

PaaS:

مزایا:

Os، سیستم‌عامل در هر زمان می‌تواند به‌روز شود.

به تیم‌های توزیع‌شده جغرافیایی اجازه می‌دهد تا اطلاعات را برای توسعه پروژه‌های نرم‌افزاری به اشتراک بگذارند.

خطرات:

مکان داده‌ها

دسترسی ممتاز

سیستم‌های توزیع‌شده

SaaS :

مزایا:

از انجا که نرم افزار بر روی سرور ارائه دهنده خدمات ابر،نگهداری می شود ؛نیاز به سخت افزار برای استقرار نرم افزار وجود ندارد.

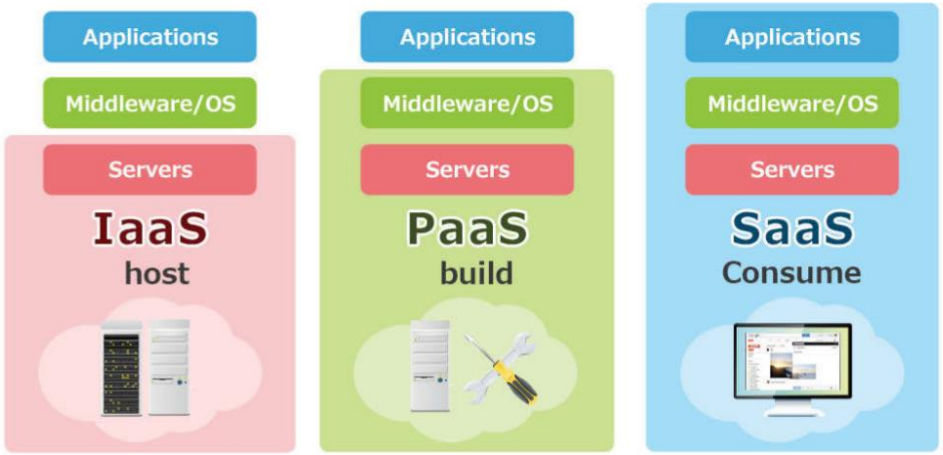
هزینه کمتر

خطرات:

محرمانه بودن داده‌ها

امنیت اطلاعات

احراز هویت و مجوز



چالش های امنیت داده:

برای تقویت امنیت در رایانش ابری، تهیه تأیید اعتبار، مجوز و کنترل دسترسی برای داده‌های ذخیره‌شده در ابر مهم است.
سه حوزه اصلی در امنیت داده‌ها عبارتند از: محرمانه بودن، تمامیت، دسترسی
از دست‌دادن داده یا نشت داده‌ها می‌تواند تأثیر جدی بر تجارت، برند و اعتماد یک سازمان داشته باشد.

سیستم باید امنیت را به‌گونه‌ای حفظ‌کند که داده‌ها فقط توسط شخص مجاز اصلاح شوند.
در محیط مبتنی بر ابر، باید یکپارچگی داده‌ها به‌درستی حفظ شود تا از دست‌رفتن داده‌ها جلوگیری شود.
به طورکلی، هر تراکنش در رایانش ابری باید خصوصیات ACID را برای حفظ یکپارچگی داده‌ها دنبال کند.

- **محل:**

در محاسبات ابری، داده‌ها در مناطق مختلفی توزیع می‌شوند
و یافتن مکان داده‌ها دشوار است. وقتی داده‌ها به مکان‌های مختلف جغرافیایی منتقل می‌شوند، قوانین حاکم برآن داده‌ها نیز می‌تواند، تغییرکند. بنابراین یک مسئله پیروی از قوانین و حفظ حریم خصوصی داده‌ها در محاسبات ابری است. مشتریان باید موقعیت مکانی اطلاعات خود را بدانند و این امکان باید از طرف ارائه‌دهنده خدمات تضمین شود.

چالش های امنیت داده:

- **دسترسی:**

در دسترس بودن مهمترین مسئله در سازمان‌های مختلف است که به عنوان یک مسئله مهم در مواجهه با خرابی با ان مواجهه هستند. در یک سازمان، بخشی از کارمندان براساس سیاست‌های امنیتی شرکت خود، به بخشی از داده‌ها دسترسی پیدا می‌کنند و سایرکارمندان شاغل در همان سازمان نمی‌توانند به همان داده‌ها دسترسی پیدا کنند. ازآنجا که دسترسی از طریق اینترنت برای همه کاربران ابری فراهم شده است؛ لازم است دسترسی ممتاز برای کاربر فراهم شود.

- **محرمانه بودن:**

داده‌ها روی سرورهای از راه‌دور توسط کاربران ابری ذخیره می‌شوند و محتوا شامل: داده‌ها، فیلم‌ها و .... می‌توانند در اختیار ارائه دهندگان یک یا چند ابر قرارگیرد.
هنگامی که داده ها در سرور راه دور ذخیره می‌شوند؛ محرمانه بودن داده‌ها یکی از ملزومات مهم است. برای محرمانه نگه‌داشتن، اطلاعات رمزنگاری می‌شوند و در طی انتقال یا جاهایی که ممکن است ذخیره شود، رمزشده باقی می‌ماند.

چالش های امنیت داده:

- **تفکیک:**

یکی از ویژگی‌های اصلی محاسبات ابری چنداجاره‌ایی بودن ان است. از آنجا که چنداجاره‌ایی بودن ابر، اجازه می‌دهد تا داده‌ها توسط چندین کاربر در سرورهای ابری ذخیره شود، امکان نفوذ وجود دارد. با واردکردن کد مشتری یا با استفاده از هر برنامه‌ایی، می‌توان داده ها را مورد حمله قرارداد؛ بنابراین این یک ضرورت است که داده‌های مشتری به صورت جداگانه ذخیره شود.

آسیب پذیری‌های که با تفکیک داده‌ها ایجاد می‌شود را می‌توان با استفاده از تست‌هایی مانند علائم تزریق SQL، اعتبارسنجی داده‌ها و ذخیره ناامن کشف کرد.

- **نقض کردن:**

شکستن داده‌ها مسئله مهم امنیتی دیگری است که باید در ابر بررسی شود.

از آنجا که داده‌های بزرگ کاربران مختلف در ابر ذخیره می‌شود، امکان دارد کاربر مخرب وارد ابر شود به گونه‌ای که کل محیط ابر مستعد حمله باشد.

تامین امنیت رایانش ابری با استفاده از رمزنگاری:

❖ **الگوریتم کلید متقارن:**
در این الگوریتم از یک کلید محرمانه (خصوصی) استفاده می‌کنند؛ که برای ارسال‌کننده و دریافت‌کننده شناخته شده است. از همان کلید خصوصی برای رمزگزاری و رمزگشایی استفاده می‌شود.
شامل: استاندارد رمزگذاری داده‌ها (DES)، استاندارد رمزگشایی پیشرفته (AES)، Triple Desi

❖ **الگوریتم کلید نامتقارن:**
از یک جفت کلید برای رمزنگاری استفاده می‌کند، یک کلید عمومی برای رمزنگاری و یک کلید خصوصی برای رمزگشایی.
این الگوریتم هزینه محاسباتی بالا و سرعت پائینی دارد.
از الگوریتم های مختلفی مانند: Shamir , Rivest , RSA ، استفاده میکند.

❖ **توابع هش:**
از یک انتقال ریاضی غیرقابل برگشت، برای تبدیل داده‌ها به یک مقدار فشرده استفاده می‌کند.
شامل الگوریتم هایی مثل: پیام Digest، الگوریتم Secure Hash است.

✓ **رمزگذاری متقارن** به عنوان راه‌حل انتخاب می‌شود؛
زیرا دارای سرعت و راندمان محاسباتی بالا برای رمزگذاری حجم زیادی از داده‌ها است.

✓ زمان لازم برای شکستن یک الگویتم رمزگذاری، ارتباط مستقیم با طول کلید مورد استفاده برای برقراری ارتباط دارد، هر چه طول کلید طولانی‌تر باشد، رمزگذاری قوی‌تر است.

الگوریتم AES:

- AES مخفف " Advanced Encryption Standard " است.
- استاندارد رمزگذاری پیشرفته، یک الگوریتم رمزگذاری متقارن است.
- مبتنی بر چندین تعویض، جایگشت و تحولات خطی است که هر یک در بلوک‌های داده ۱۶بایت اجرا می‌شوند.
- هنگامی که می خواهیم متن محرمانه‌ای را با فرمت رمزگشایی، رمزگذاری کنیم این الگوریتم مفید است.
(رمزگشایی متن رمزگذاری شده فقط درصورتی امکان‌پذیر است که رمز عبور مناسب را بدانیم.)
- الگوریتم AES، حداقل زمان را برای رمزگذاری مصرف می‌کند و RSA طولانی‌ترین زمان رمزگذاری را مصرف می‌کند.
- هیچ حمله عملی علیه AES وجود ندارد؛ بنابراین بهترین الگوریتم رمزگذاری برای دولت‌ها، بانک‌ها و سیستم-های نیازمند امنیت بالا در سراسرجهان است.

الگوریتم AES:

داده ها در طی چندین مرحله به یک پیام ایمن تبدیل خواهند شد. این‌کار با هر بلوک متنی ساده و دارای اندازه‌ای استاندارد آغاز می‌شود. پیام در قالب یک آرایه قرار گرفته و سپس فرآیند رمزنگاری بر روی پیام اجرا می‌شود. در هر دور از رمزنگاری، اعمال جایگزینی، انتقال و ترکیب پیاده‌سازی خواهند شد.

AES بر مبنای رمزنگاری بلوکی عمل می‌کند و اندازه هر بلوک در آن معادل با ۱۲۸ بیت است. کلیدها متقارن بوده و در ۳ اندازه مختلف ۱۲۸، ۱۹۲ یا ۲۵۶ بیتی قابل‌دسترس هستند. فرآیند رمزنگاری برای کلید ۱۲۸ بیتی شامل ۱۰ مرحله، برای کلید ۱۹۲ بیتی شامل ۱۲ مرحله و برای کلید ۲۵۶ بیتی دارای ۱۴ مرحله خواهد بود

مرحله اول:

- Add Round Key

مرحله دوم:

- Sub Bytes
- Shift Rows
- Mix Columns
- Add Round Key

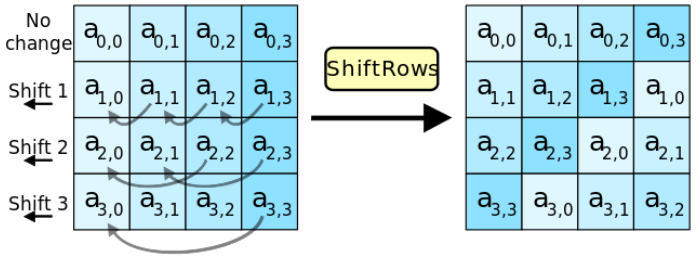
مرحله اخر:

- Sub Byte
- Shift Row
- Add Round Key

الگوریتم AES:

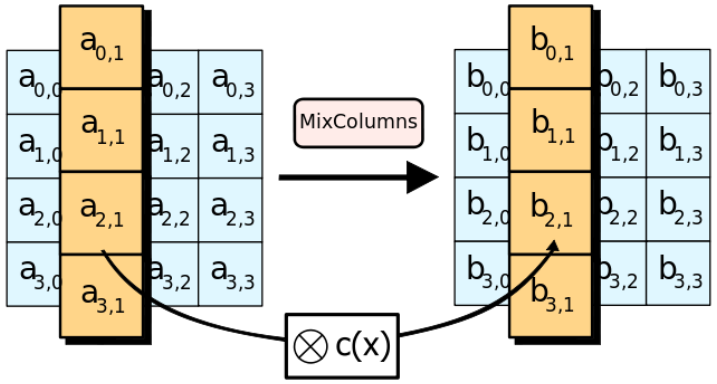
جابه‌جایی سطرها (Shift Rows):

در SubBytes هر بایت در state با مقداری در جدول جستجو با ۸ بیت ثابت جایگزین می‌شود



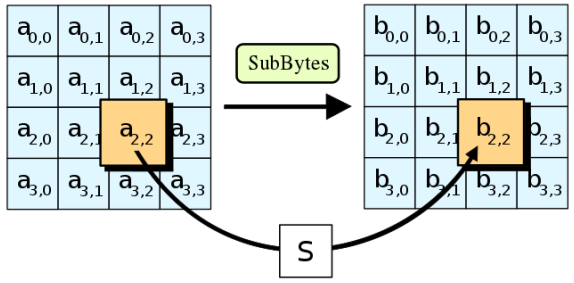
ترکیب ستون‌ها (Mix Columns)

در مرحله MixColumns هر ستون از state با یک چندجمله‌ای C(x) ضرب می‌شود.



تعویض بایت (Sub Bytes)

هر یک از چهار ردیف ماتریس به سمت چپ منتقل می‌شوند. هر ورودی که "سقوط کند" در سمت راست سطر دوباره وارد می‌شود



نتیجه گیری:

با استفاده از رایانش ابری ،کاربران میتوانند از طریق هر کامپیوتری که به اینترنت متصل باشد به داده ها و برنامه کاربردی خود دسترسی داشته باشند. از طرفی رایانه ایی که کاربران با ان به ابر دسترسی پیدا می کنند، می تواند رایانه ایی ارزان قیمت و نه چندان قدرمند باشد؛ این دسترسی میتواند از طریق لب تاپ، تبلت و حتی موبایل نیز انجام گیرد.

امنیت و حفظ حریم خصوصی به دلیل داشتن اطلاعات حساس و مهم ذخیره شده در ابر برای مشتریان، به عنوان یک مسئله مهم در محیط محاسبات ابری مطرح است و تامین امنیت داده ها از وظایف مهم ارائه دهندگان خدمات رایانش ابری است.

برای فراهم کردن دسترسی ایمن به داده‌ها در ابر، می‌توان از روش‌های پیشرفته رمزگذاری برای ذخیره و بازیابی داده‌ها از ابر استفاده کرد.

رمزگذاری AES از سطح امنیتی بسیار بالایی برخوردار است.
AES، سریع‌ترین روشی است که قابلیت انعطاف‌پذیری و مقیاس پذیری را دارد و به‌راحتی اجرا می‌شود؛ در این رمزگذاری، حداقل فضا برای ذخیره‌سازی استفاده می‌شود و می‌توان گفت بدون هیچ‌گونه ضعف و محدودیت است.