Scientific Journal of Passive Defence
Vol. 14, No. 4, Winter 2023, Serial No. 56
ISSN: 2980-8030 , E-ISSN: 2008-6849

The Latest Classification of Cloud Computing Security Issues: Challenges, Attacks and Solutions

S. Gavidel , M. Naghavi *, D. Asgharzadeh

*Assistant Professor, Computer Faculty, Imam Hossein University, Tehran, Iran
(Received: 13/03/2023, Revised: 04/04/2023, Accepted: 07/08/2023, Published: 22/12/2023)
DOR: 20.1001.1.20086849.1402.14.4.10.6

ABSTRACT

cloud computing has revolutionized internet service with its advent. in cloud computing, security is the most important goal and the main requirement of a system. as cloud computing develops, a set of security problems appears. security problems are a strong obstacle to the adaptation of users to cloud computing systems. cloud security is becoming a key distinction and competitive advantage between cloud providers. this paper presents some cloud computing systems and analyzes the problem of cloud computing and its strategy with regard to the concepts and features of cloud computing. this paper tries to provide a comprehensive overview of cloud computing security and some of the key research challenges of cloud computing security. in this paper, the latest and most important cloud security issues such as data security, data secrecy, program security and challenges, attacks and solutions to deal with them with the development of cloud computing have been discussed. in the end, special security issues including the identity of access credit, development of insecure software, and third- party sources were investigated.

Keywords: Cloud Computing, Cloud Computing Security, Cloud Computing Challeng, Countering Attacks on Cloud Comp

* Corresponding Author Email: mnaghavi@ihu.ac.ir

نشریه علمی پدافند غیرعامل

سال چهاردهم، شماره ۴، زمستان ۱۴۰۲، (پیاپی ۵۶): صص ۱۲۷-۱۱۱

علمی – ترویجی

شاپای چاپی: ۶۹۴۹-۲۰۰۸ | شاپای الکترونیکی: ۸۰۳۰-۲۹۸۰

ارائه جدیدترین طبقه‌بندی مسائل امنیتی رایانش ابری : چالش‌ها، حمله‌ها، راه‌حل‌ها

سجاد قویدل[۱]، مهدی نقوی[۲*]، داود اصغرزاده[۳]

DOR: 20.1001.1.20086849.1402.14.4.10.6

تاریخ دریافت: ۱۴۰۱/۱۲/۲۲ تاریخ پذیرش: ۱۴۰۲/۰۵/۱۶

تاریخ بازنگری: ۱۴۰۲/۰۱/۱۵ تاریخ انتشار: ۱۴۰۲/۱۰/۰۱

چکیده

رایانش ابری با ظهور خود انقلابی در خدمات‌دهی اینترنت به وجود آورده است. در رایانش ابری مسئله امنیت مهم‌ترین هدف و نیاز اصلی یک سیستم می‌باشد. با توسعه رایانش ابری، مجموعه‌ای از مشکلات امنیتی ظاهر شده است. وجود مسائل امنیتی مانعی قوی برای سازگاری کاربران با سیستم‌های رایانش ابری است. امنیت ابری در حال تبدیل شدن به یک تمایز کلیدی و مزیت رقابتی بین ارائه دهندگان ابر است. این مقاله برخی از سیستم‌های رایانش ابری را معرفی می‌کند و مشکل امنیت رایانش ابری و راهبرد آن را با توجه به مفاهیم و نمادهای رایانش ابری تحلیل می‌کند، سعی شده است این مقاله نگاهی جامع به امنیت رایانش ابری داشته باشد و مسائل مربوط به امنیت رایانش ابری و برخی از چالش‌های تحقیقاتی کلیدی پیاده‌سازی راه‌حل‌های امنیتی ابری بررسی شده است. در این مقاله به جدیدترین و مهم‌ترین مسائل امنیتی ابر مانند امنیت داده، محرمانگی داده، امنیت برنامه و چالش‌ها، حمله‌ها و راه‌حل‌های مقابله با آن‌ها با توسعه رایانش ابری پرداخته شده است. در انتها مسائل امنیتی خاص ابر شامل هویت اعتبار دسترسی، توسعه نرم‌افزار ناامن، منابع شخص ثالث ناامن مورد بررسی قرار گرفت.

کلیدواژه‌ها: رایانش ابری، امنیت رایانش ابری ، چالش‌های رایانش ابری، مقابله با حملات به رایانش ابری

[۱] دانشجوی کارشناسی ارشد دانشکده هوش مصنوعی وعلوم شناختی، دانشگاه جامع امام حسین (ع)، ایران، تهران

[۲] استادیار دانشکده کامپیوتر دانشگاه جامع امام حسین (ع)، ایران، تهران (mnaghavi@ihu.ac.ir)- نویسنده مسئول

[۳] دانشجوی کارشناسی ارشد دانشکده هوش مصنوعی وعلوم شناختی، دانشگاه جامع امام حسین (ع)، ایران، تهران

۱- مقدمه

رایانش ابری یکی از فناوری‌های مهم درسیستم‌های فناوری اطلاعات است. این فناوری دارای ویژگی‌های جدید است که آن را از سایر فناوری‌های فناوری اطلاعات متمایز می‌کند. منابع و فضای اطلاعاتی به صورت پویا میان کاربرهای مختلف، به اشتراک گذاشته شده و ازحداکثر توان سخت افزار برای خدمت رسانی به ابرهای مختلف استفاده می‌شود. امنیت یکی از مهم‌ترین موضوع‌های رایانش ابری می‌باشد. اگر سازمانی یا شرکتی احساس امنیت نداشته باشد داده‌ها واطلاعات خودرا در ذخیره‌سازهای سامانه رایانش ابری به اشتراک نمی‌گذارد و این یک تهدید در این فناوری به حساب می‌آید [۱].

گارتنر رایانش ابری را سبکی از رایانش تعریف می‌کند که در آن قابلیت‌های مبتنی بر فناوری اطلاعات، در مقیاس بزرگ و به عنوان خدمات در اختیار کاربران اینترنت قرار می‌گیرد. نکته کلیدی در [۱] این تعریف، اصطلاح «به‌عنوان خدمت» است که به پرداخت هزینه و تعریف قراردادهای سطح خدمت اشاره دارد.

۱-۱- فرصت‌های امنیت رایانش ابری

طبق اعلام گارتنر در سال ۲۰۲۳ میلادی[۱۸] در خصوص چشم انداز امنیت ابری و راهبردهای آن، فرصت‌های امنیت رایانش ابری در ۵ عنوان به صورت زیر اعلام شده است:

الف) نقش معماری امنیت ابر و معمار امنیت ابر کلید موفقیت ابتکارات رایانش ابری است زیرا ابر به مجموعه متفاوتی از اصول، فرآیندها و فناوری‌های طراحی امنیتی نیاز دارد.

ب) ارزیابی احتمال خطر ابری باید به صورت خودکار انجام شود تا با نیازهای تجاری همگام شود.

پ) ارائه دهندگان ابر سطح ۱معمولاً نقاط شروع امن‌تر برای بارهای کاری از همه نوع هستند.

ت) بسیاری از شرکت‌ها یک راهبرد چند ابری را اتخاذ کرده‌اند که استفاده از ابزارهای امنیتی شخص ثالث را برای سیاست‌گذاری و حاکمیت منسجم در یک چشم‌انداز چند ابری ضروری می‌کند.

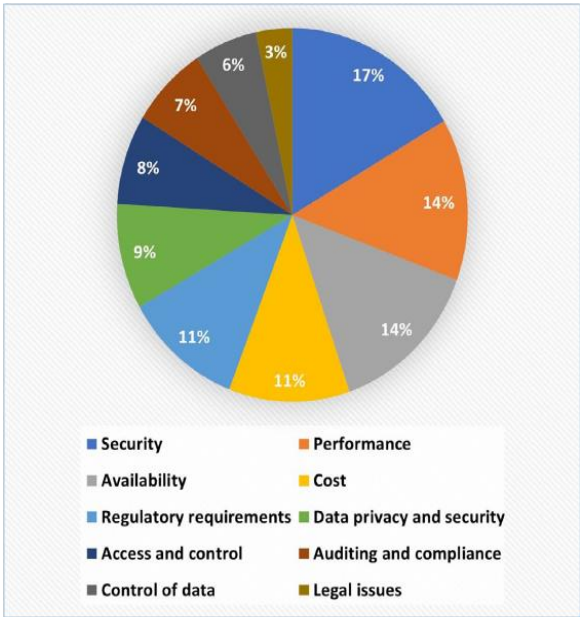
ث) کاربران نهایی به طور فزاینده‌ای از صدها نرم‌افزار به عنوان برنامه‌های کاربردی خدمات و زیرساخت‌های متعدد به عنوان ارائه خدمات استفاده می‌کنند و با استفاده از پلتفرم به عنوان فناوری خدمات، خدمات جدیدی را ایجاد می‌کنند .بنابراین، ابتکارات امنیت ابری باید «عوامل شکل» مختلف ابری را که توسط بسیاری از سازمان‌ها استفاده می‌شود، در نظر بگیرد.

۱-۲- روش تحقیق

با بررسی پژوهش‌هایی که در خصوص مسائلی که در حوزه رایانش ابری انجام شده است طبق شکل (۱) امنیت رایانش ابری با ۱۷ ٪ به‌عنوان مهم‌ترین مسئله رایانش ابری را به خود اختصاص داده است. به همین علت مطالعاتی که درحوزه امنیت رایانش ابری انجام پذیرفته براساس نتایج آن به عنوان جدیدترین مطالعات انجام شده تحت عنوان زیست‌بوم امنیت رایانش ابری در شکل (۳) آورده شده است.

۲- مفاهیم پایه

مفاهیم پایه شامل مدل‌های استقرار ابری، مدل‌های خدمات ابری، ویژگی‌های اساسی ابری، چالش‌های امنیتی ابری، مهم‌ترین مسائل امنیتی ابری، مسائل امنیتی خاص ابری، انواع حملات ابری و روش‌های حفاظت به‌طور خلاصه تشریح می‌شوند.

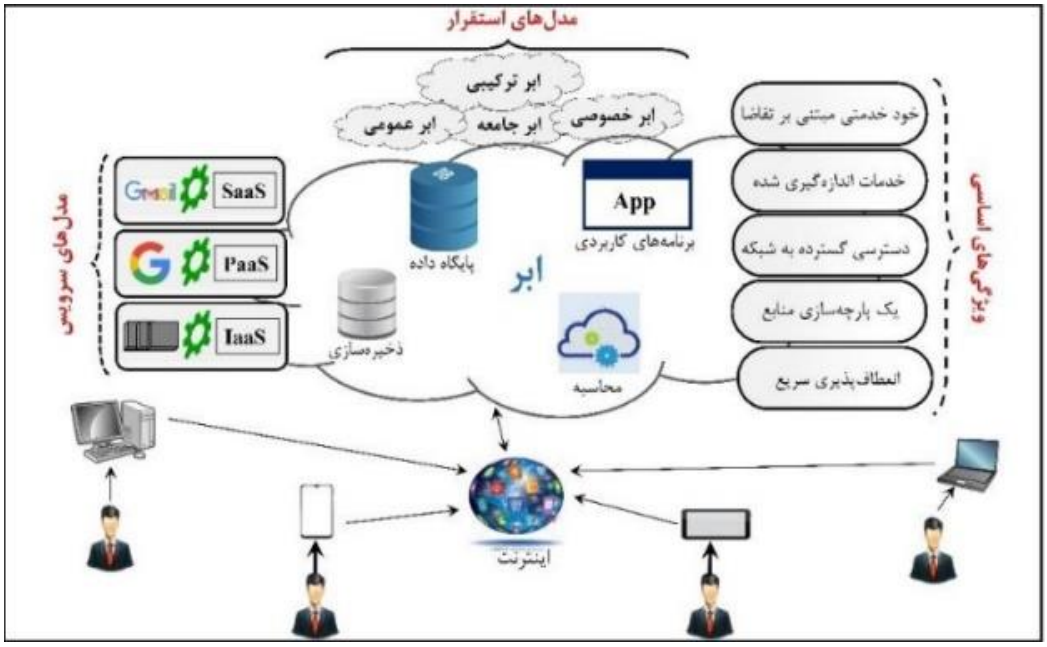


شکل (۱): تجزیه و تحلیل مسائل مختلف درگیر در محیط ابری[۱۰]

۲-۱- مدل‌های استقرار ابری

در خصوص نحوه شکل‌گیری رایانش ابری می‌توان به، پنج مدل استقرار ابر که تاکنون مورد بحث قرار گرفته است اشاره کرد. که عبارتند از: ابر عمومی، خصوصی، ترکیبی، اجتماعی و مجازی خصوصی (VPC[1]) هستند. در میان این مدل‌ها VPC کمتر مورد توجه جامعه پژوهش قرار گرفته است. ویژگی‌های این مدل‌های استقرار در جدول(۱) وشکل (۲) خلاصه شده است[۴].

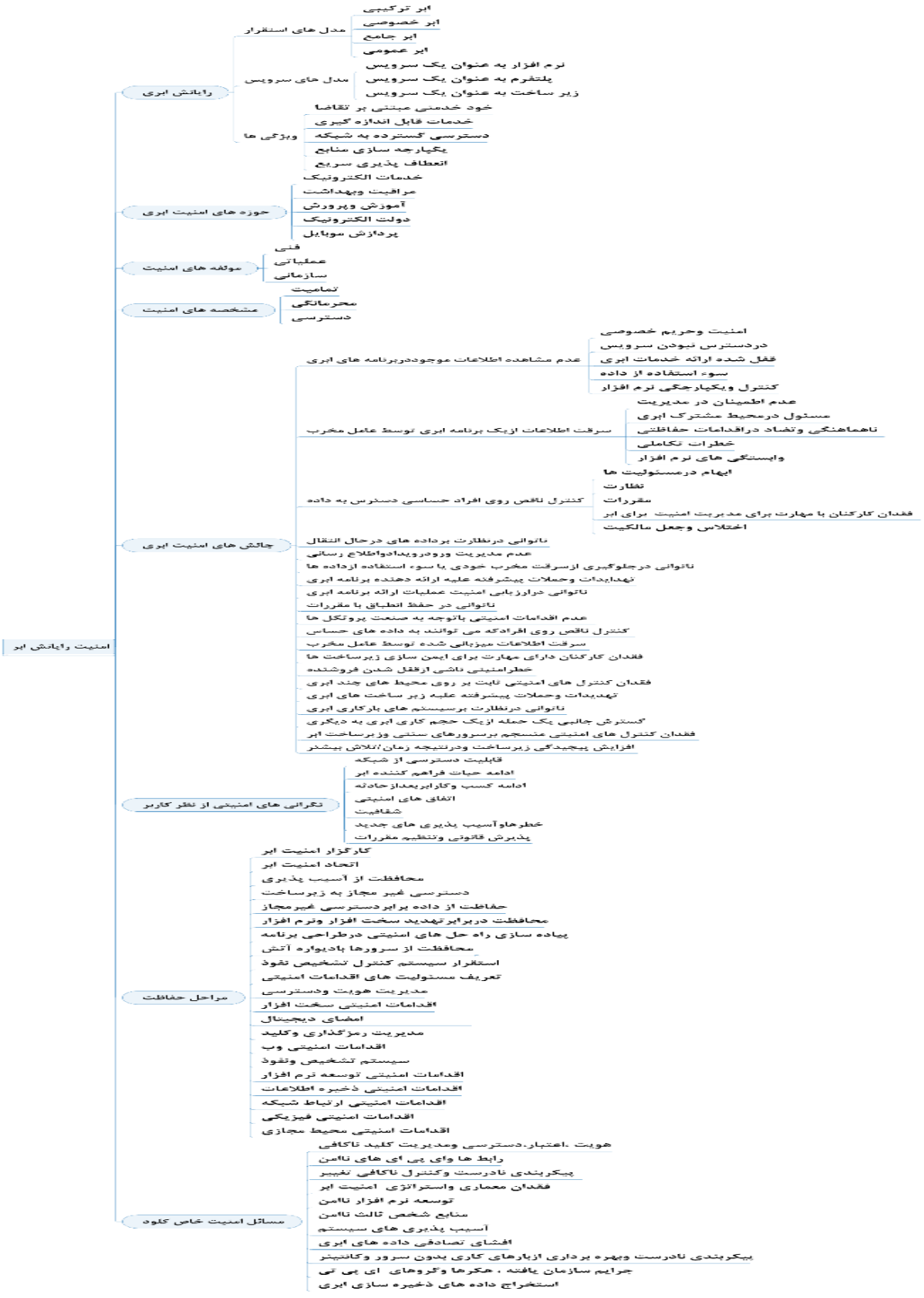
[1]Virtual Port Channel



شکل (۲): رایانش ابری در تصویر[۲]

جدول (۱): مدل‌های استقرار ابری[۱۱]

مدل استقرا	ویژگی‌ها
ابر عمومی	در این مدل با دسترسی کاربران به اینترنت برای دریافت خدمات، رایانش ابری خدمات خود را برای کاربران نهایی فراهم می‌کند. بنابراین، این خدمات ابری به صورت عمومی قابل دسترسی هستند. ارائه دهنده خدمات ابری زیرساخت‌های مورد نیاز را برای کاربران نهایی فراهم می‌کند.
ابر خصوصی	این مدل در سازمان‌ها برای برآوردن نیازهای ابری در سطوح مختلف در سازمان‌ها استفاده می‌شود. آنها زیرساخت خود را برای راه‌اندازی خدمات‌های ابری حفظ خواهند کرد. این مدل، هزینه استفاده از خدمات ابری برای سازمان را در درازمدت با امنیت بیشتر کاهش می‌دهد، زیرا مدل‌های ابر خصوصی در شبکه‌های خصوصی در پشت دیواره‌های آتش خود مستقر می‌شوند.
ابر جامعه	مدلی است که برای استقرار زیرساخت ابری استفاده می‌شود که می‌تواند بین چندین سازمان با اهداف مشابه به اشتراک گذاشته شود. قابل مقایسه با ابر خصوصی است اما در بین برخی سازمان‌ها به اشتراک گذاشته شده است.
ابر هیبریدی	مدل ابر ترکیبی از دو یا چند مدل از مدل‌های فوق (به ویژه ابر عمومی و خصوصی) تشکیل شده است. دارای زیرساخت‌های منفرد و موجودیت‌های منحصر به فردی می‌باشد، و توسط فناوری‌های استاندارد یا اختصاصی به هم متصل می‌شوند. و امکان انتقال داده‌ها و برنامه‌های کاربردی را بین زیرساخت‌های متصل به هم را فراهم می‌کند. هدف از این شکل، ترکیبی از خدمات و ایجاد راه‌حلی است که به بهترین وجه نیازهای مشخص هر شرکت را برآورده کند. برای مثال، یک مشتری ابری می‌تواند حجم کاری حیاتی را در یک ابر خصوصی اجرا کند، اما از خدمات پایگاه‌داده یک ارائه دهنده ابر عمومی برا ی داده‌های غیر حیاتی استفاده کند.
ابر خصوصی مجازی	مدل ابر خصوصی مجازی اصطلاح «ابر خصوصی مجازی» برای اولین بار توسط خدمات وب آمازون در زمان معرفی محصول جدید آن «VPC Amazon» به طور گسترده مورد استفاده قرار گرفت. در مدل ابر خصوصی مجازی، ارائه دهنده ابر زیرساخت‌های زیر بنایی را منحصرا برای یک سازمان فراهم می‌کند که می‌تواند شامل تعدادی کاربر(به‌عنوان مثال، بخش‌های تجاری) باشد.



شکل (۳): زیست بوم امنیت رایانش ابری

۲-۲- مدل‌های خدمات ابر به شرح زیر است :

رایانش ابری خدمات خودرا به سه شکل ارائه می‌دهد که به‌صورت زیر می‌باشد[۵].

۲-۲-۱- نرم‌افزار به عنوان خدمت (SaaS)

این یک مدل تحویل نرم‌افزار "یک به چند" است که به برنامه‌ها از طریق خدمات شبکه دسترسی می‌دهد. و کاربران می‌توانند هر چیزی را در محل خود نصب کنند و هزینه اولیه قابل توجهی را برای خرید نرم‌افزار و مجوز مورد نیاز باید بپردازند. و آنها طبیعتاً به‌عنوان مستاجر هستند. کاربران مجبور نیستند که پایگاه ابری اساسی شامل شبکه، سرورها، سیستم‌عامل‌ها، ذخیره‌سازی و غیره را کنترل کنند. و به‌روزرسانی به‌صورت خودکار انجام می‌شود و دارای پلتفرم مستقل است. محبوب‌ترین‌هایsaas مورد استفاده عبارتند از: Google، Google Drive، Microsoft Office و غیره.

۲-۲-۲- پلتفرم به عنوان خدمت (PaaS[1])

PaaS یک پلتفرم توسعه و استقرار برای اجرای برنامه‌های کاربردی در فضای ابری است که از یک محیط زبان برنامه‌نویسی، سیستم عامل، وب سرور و پایگاه داده تشکیل شده است. کاربران داده‌ها و منابع برنامه را مدیریت می‌کنند در حالی که سایر منابع توسط ارائه دهندگان ابری مدیریت می‌شوند. PaaS مقیاس‌پذیر و کم هزینه و همچنین دامنه برای توسعه‌دهندگان است. ارائه دهندگان محبوب PaaS عبارتند از: Windows Azure، Heroku، Google App Engine و غیره.

۲-۲-۳- زیرساخت به‌عنوان خدمت (IaaS[2])

IaaS محبوب‌ترین و رشد یافته‌ترین بخش بازار محاسبات ابری می‌باشد. و پردازش، ذخیره‌سازی، ظرفیت شبکه و سایر موارد اساسی را به‌کار می‌گیرد. و همچنین منابع محاسباتی خدمات معماری و زیرساخت محاسباتی و همچنین منابع محاسبات مجازی را ارائه می‌دهد. که کاربران مختلف می‌توانند به آنها دسترسی داشته باشند. عمدتا توسط مدیران سیستم استفاده می‌شود. IaaS محبوب مورد استفاده خواهد بود. Amazon، GoGrid و غیره.

۳- ویژگی‌های اساسی رایانش ابری

مهم‌ترین ویژگی‌های که می‌توان برای رایانش ابری بیان کرد به شرح ذیل می‌باشد[۹].

- **خدمت بر حسب تقاضا**: مصرف‌کننده می‌تواند به طور یک جانبه قابلیت‌های محاسباتی مانند زمان سرور و ذخیره‌سازی شبکه را در صورت نیاز به صورت خودکار ارائه دهد.
- **دسترسی گسترده به شبکه**: کلیه خدمات در رایانش ابری از طریق شبکه در دسترس هستند و توسط دستگاه‌های مختلف مانند رایانه رومیزی، تلفن‌همراه، تلفن‌های هوشمند و دستگاه‌های تبلت قابل دسترسی هستند.
- **تجمیع منابع:** منابع محاسباتی ارائه دهنده برای ارائه خدمات به چندین مصرف‌کننده با استفاده از یک مدل چند مستاجر، فیزیکی و متفاوت ترکیب می‌شوند.

۴- چالش‌های امنیتی رایانش ابری

ابر چندین مزیت را برای سازمان‌ها فراهم می‌کند. با این‌حال، تهدیدات و نگرانی‌های امنیتی خاص خود را نیز به‌همراه دارد. زیرساخت‌های مبتنی‌بر ابر با یک مرکز داده داخلی بسیار متفاوت است و ابزارها و راهبردهای امنیتی سنتی همیشه قادر به ایمن سازی موثر آن نیستند. در جدول (۲) به مسائل مهم و تهدیدات امنیتی ابری اشاره می‌شود[۱۷].

جدول (۲): مهمترین چالش‌های رایانش ابری در سال ۲۰۲۲ [۱۷]

ردیف	مسائل
	چالش‌های مربوط به SaaS
۱	سرقت اطلاعات از یک برنامه ابری توسط عامل مخرب
۲	کنترل ناقص روی افرادی که می‌توانند به داده‌های حساس دسترسی داشته باشند
۳	ناتوانی در نظارت بر داده‌های در حال انتقال از برنامه‌های ابری
۴	برنامه‌های ابری که خارج از قابلیت نظارت IT ارائه می‌شوند (به عنوان مثال، IT سایه)
۵	فقدان مهارت کارکنان مدیریت امنیت برای برنامه‌های ابری
۶	ناتوانی در جلوگیری از سرقت مخرب خودی یا سوء استفاده از داده‌ها
۷	تهدیدات و حملات پیشرفته علیه ارائه دهنده برنامه ابری
۸	ناتوانی در ارزیابی امنیت عملیات ارائه دهنده برنامه ابری
۹	عدم اطلاع از برنامه‌های کاربردی داخل رایانش ابری
۱۰	ناتوانی در حفظ انطباق با مقررات
	چالش‌های مربوط به IaaS
۱۱	حجم‌های کاری ابری و حساب‌هایی که خارج از قابلیت تحلیل و بررسی فناوری اطلاعات ایجاد می‌شوند (به عنوان

[1] Platform as a service
[2] Infrastructure as a Service

جدول (۲): مهمترین چالش‌های رایانش ابری در سال ۲۰۲۲ [۱۷]

ردیف	مسائل
	مثال، IT سایه)
۱۲	سرقت اطلاعات میزبانی شده در زیر ساخت ابری توسط عامل مخرب
۱۳	فقدان کارکنان دارای مهارت برای ایمن‌سازی زیر ساخت‌های ابری
۱۴	تهدیدات و حملات پیشرفته علیه زیر ساخت‌های ابر
۱۵	ناتوانی در جلوگیری از سرقت مخرب خودی یا سوء استفاده از داده‌ها
۱۶	فقدان کنترل‌های امنیتی ثابت بر روی محیط‌های چند ابری و داخلی
۱۷	ناتوانی در نظارت بر سیستم‌های بار کاری ابری و برنامه‌های کاربردی برای آسیب‌پذیری‌ها
۱۸	گسترش جانبی یک حمله از یک حجم کاری ابری به دیگری
	چالش‌های مربوط به ابر خصوصی
۱۹	فقدان کنترل‌های امنیتی منسجم بر سرورهای سنتی و زیر ساخت‌های ابر خصوصی مجازی‌سازی شده
۲۰	افزایش پیچیدگی زیرساخت و در نتیجه زمان/تلاش بیشتر برای اجرا و نگهداری آن
۲۱	فقدان کارکنان دارای مهارت برای مدیریت امنیت برای یک مرکز داده تعریف شده با نرم‌افزار (مانند محاسبات مجازی، شبکه، ذخیره‌سازی)
۲۲	مشاهده ناقص امنیت برای یک مرکز داده تعریف شده توسط نرم‌افزار (به‌عنوان مثال، محاسبات مجازی، شبکه، ذخیره‌سازی)
۲۳	تهدیدات و حملات پیشرفته

۵- مهم‌ترین مسائل امنیتی

مهم‌ترین مسائل امنیتی که رایانش ابری با آن مواجه است به شرح زیر می‌باشد [۵] :

۵-۱- امنیت داده‌ها

داده یکی از مهمترین سرمایه یک سازمان یا کاربر می‌باشد. به همین دلیل بعنوان اولویت اول در مسئله امنیت رایانش ابری به حساب می‌آید. امنیت داده حیاتی‌ترین چالش برای هر مدل ابری است. Saas users باید به ویژگی‌های امنیتی ارائه شده توسط ارائه دهندگان خدمات ابری خود برای اطمینان از محافظت از داده‌ها اعتماد کنند. در مدل خدمات Saas، داده‌ها در مراکز داده ارائه دهنده ذخیره می‌شوند و از دیواره‌های آتش برای محافظت از این اطلاعات حساس استفاده می‌شود. علاوه بر این، ارائه دهندگان باید امنیت بیشتری را در برابر نقض‌های داده‌ای که توسط نرم‌افزارهای مخرب یا کارمندان انجام می‌شود، افزایش دهند. این وظیفه ارائه دهنده خدمات Cloud است که محیط ابری ایمن را تضمین کند.

۵-۲- امنیت برنامه

در واقع هر کاربر یا سازمان خدمات خود را در قالب برنامه در اختیار درخواست کننده قرار می‌دهد و در واقع برنامه‌های ابری عمدتاً از طریق مرورگرهای وب ارائه می‌شوند. و همچنین ممکن است برای ارائه خدمات از برنامه‌های کاربردی هم مورد استفاده قرار بگیرند. برنامه‌های کاربردی ابری عمدتاً از طریق مرورگرهای وب ارائه می‌شوند. هکرها اغلب از ابزارهای وب برای حمله به رایانه‌های کاربر برای انجام فعالیت‌های مخرب مانند سرقت اطلاعات خصوصی استفاده می‌کنند. فقدان امنیت در برنامه وب ممکن است برنامه‌های Saas را آسیب‌پذیر کند.

۵-۳- دسترسی

مهم‌ترین مزیت یک برنامه در دسترس بودن آن است به همین دلیل یکی از مزیت‌های اصلی نرم‌افزار به عنوان یک خدمت این است که می‌توان در هر جایی که اتصال اینترنتی از طریق دستگاه‌های تلفن‌همراه و رایانه وجود دارد، به آن دسترسی داشت. با وجود اینکه راحتی کاربر را افزایش می‌دهد، اما خطر بزرگی را نیز به همراه دارد. (CSA)[1] گزارشی را در مورد محاسبات تلفن‌همراه و تهدیدات آن مانند بدافزارهای مخربی که اطلاعات را سرقت می‌کنند، شبکه‌های ناامن، هک مبتنی بر مجاورت و نقص در سیستم عامل دستگاه منتشر کرده است.

۵-۴- یکپارچگی داده

درحالتی که داده‌ها به صورت یکپارچه باشند میزان درستی و سالمی آن داده می‌باشد در واقع یکپارچگی داده تضمین می‌کند که داده‌ها خراب نیستند و فقط توسط یک شخص مجاز قابل دسترسی و اصلاح هستند. این به‌عنوان "سطحی که مجموعه‌ای از داده‌ها کامل، سازگار و دقیق است" تعریف می‌شود. حفظ یکپارچگی داده‌ها برای اطمینان از استفاده از داده‌ها برای انتخاب خوب و ارائه محصول با کیفیت بسیار مهم است. یکپارچگی داده

[1] CloudSecurity Alliance

را می‌توان با اطمینان از رعایت اصل ALCOA (ویژگی خوانا، همزمان، اصلی و دقیق) به‌دست آورد.

۵-۵- محرمانه بودن داده‌ها

داده زمانی پر اهمیت و مهم می‌باشد که محرمانگی خود را از دست ندهد به‌همین دلیل. محرمانه بودن داده‌ها به‌عنوان جلوگیری از افشای اطلاعات به‌صورت عمدی یا غیرعمدی تعریف می‌شود. محیط ذخیره‌سازی ابری شامل سایت‌های حقوق مالکیت معنوی، کانال‌های مخفی، تجزیه و تحلیل ترافیک، رمزگذاری و ضبط است. رایانش ابری شامل اشتراک‌گذاری یا ذخیره اطلاعات روی سرورهای راه دور متعلق به کاربر یا استفاده توسط دیگران در حین دسترسی به اینترنت یا سایر ارتباطات است. در خدمات رایانش ابری تغییراتی وجود دارد. از جمله سایت‌های ذخیره‌سازی داده‌ها، سایت‌های ویدئویی، سایت‌های تهیه مالیات، وب‌سایت‌های ثبت سلامت و موارد دیگر. تمام محتویات یک دستگاه ذخیره‌سازی کاربر را می‌توان با یک ارائه دهنده ابر یا با چندین ارائه دهنده ابر ذخیره کرد. حریم خصوصی و محرمانگی هر زمان که یک فرد، کسب‌وکار، آژانس دولتی یا سازمان دیگری اطلاعاتی را در فضای ابری به اشتراک بگذارد ضروری است.

۵-۶- سرقت حساب

هر کاربر یا سازمان دارای یک حساب اختصاصی می‌باشد و در حالتی ممکن است این خطر وجود داشته باشد که حساب‌های کاربران توسط هکرها ربوده شده یا از طریق اعمال مخرب و غیرمجاز به سرقت رفته باشد. آنها ممکن است این کار را برای منافع شخصی انجام دهند، داده‌های کاربر را دستکاری کنند یا اطلاعات نادرست ارائه دهند. در SaaS، هر کسی می‌تواند به عنوان کاربر خدمات ابری ثبت نام کند، بنابراین احتمال سرقت یک حساب کاربری بسیار زیاد است.

۵-۷- امنیت شبکه

تبادل اطلاعات و داده‌ها در بین کاربران و سازمان‌ها بستگی به امنیت شبکه دارد و در مدل ابری SaaS، اطلاعات حساس از طریق برنامه Saas از شرکت‌ها در دسترس است و آنها در انتهای ارائه دهنده SaaS ذخیره می‌شوند. این داده‌های حساس از طریق شبکه قابل دسترسی هستند و بنابراین رمزگذاری جریان داده‌ها در شبکه برای جلوگیری از نشت داده‌ها مورد نیاز است. فن‌های رمزگذاری رایج مورد استفاده برای ترافیک شبکه عبارتند از (SSL)[1] و (TLS)[2].

۵-۸- تفکیک داده‌ها

ممکن است چند کاربر در ابر یک خدمت را اجاره کرده و به جداکردن، داده‌های خود را در آن مکان ذخیره کند. اجاره چندگانه یکی از اجزای مهم رایانش ابری است. به دلیل چند اجاره‌ای بودن، چندین کاربر می‌توانند داده‌های خود را با استفاده از برنامه‌های ارائه شده توسط SaaS Provider ذخیره کنند. در این موارد، داده‌های چند کاربر در یک مکان ذخیره می‌شود. به این دلیل نفوذ به داده‌های خصوصی کاربر توسط کاربر دیگری امکان‌پذیر می‌شود. با تزریق کد مشتری می‌توان بر آن غلبه کرد. بنابراین یک SaaSmodel باید یک محدودیت واضح برای داده‌های هر کاربر تضمین کند. این محدودیت نه تنها در سطح فیزیکی بلکه در سطح برنامه نیز باید تضمین شود. این خدمت باید به اندازه کافی کارآمد باشد تا داده‌ها را از کاربران مختلف جدا کند.

۵-۹- پشتیبان‌گیری

به دلیل شرایط حساس در ابر باید به طور منظم از اطلاعات و داده‌های کاربر و سازمان پشتیبان‌گیری انجام شود و این مسئولیت ارائه‌دهنده SaaS است که اطمینان حاصل کند که از تمام داده‌های حساس به‌طور منظم نسخه پشتیبان تهیه می‌شود تا در صورت بروز هر گونه خرابی، فرآیند بازیابی هموار شود. روش‌های پشتیبان‌گیری سنتی برای برنامه‌ها و مراکز داده که عمدتاً برای برنامه‌های کاربردی وب و مصرف‌کننده طراحی شده‌اند، استفاده می‌شوند، اما روش‌های پشتیبان‌گیری بهینه برای برنامه‌های کاربردی ابری نیستند. همچنین، برای جلوگیری از نشت غیرمنتظره داده‌های حساس، استفاده از یک روش رمزگذاری قوی برای ذخیره داده‌های پشتیبان ضروری است. برخی از ارائه دهندگان خدمات ابری مانند آمازون این رمزگذاری را به طور پیش فرض ارائه نمی‌کنند. بنابراین، کاربران باید به طور مستقل داده‌ها را رمزگذاری کنند تا دسترسی غیرمجاز دیگران را محدود کنند.

۶- مسائل امنیتی خاص ابر

در جدیدترین نظرسنجی که در سال ۲۰۲۲ بیش از۷۰۰ متخصص صنعت در مورد مسائل امنیتی در صنعت ابر را بررسی

[1] Secure SocketLayer
[2] Transport Layer Security

کرده‌اند. و مورد نظرسنجی قرار گرفت و پاسخ دهندگان یازده موضوع امنیتی مهم را در محیط‌های ابری شناسایی کردند. و یازده مورد طبق جدول (۳) می‌باشد[۳].

جدول (۳): نظر سنجی مسائل امنیتی خاص ابر در سال ۲۰۲۲ [۳]

#	نظرسنجی	رتبه میانگین نتایج
۱	شناسه، اعتبار، دسترسی و کلید Mgt، حساب‌های ممتاز ناکافی است	7.729927
۲	رابط ها و APIهای ناامن	7.592701
۳	پیکربندی نادرست و کنترل ناکافی تغییر	7.424818
۴	فقدان معماری و استراتژی امنیت ابری	7.408759
۵	توسعه نرم افزار ناامن	7.275912
۶	منابع شخص ثالث ناامن	7.214493
۷	آسیب پذیری های سیستم	7.143066
۸	افشای / افشای تصادفی داده های ابری	7.114659
۹	پیکربندی نادرست و بهره برداری از بارهای کاری بدون سرور و کانتینر	7.097810
۱۰	جرایم سازمان یافته / هکرها / APT	7.088534
۱۱	استخراج داده های ذخیره سازی ابری	7.085631

۶-۱- هویت، اعتبار دسترسی و مدیریت کلید ناکافی

هویت، اعتبار، سیستم‌های مدیریت دسترسی شامل ابزارها و سیاست‌هایی است که به سازمان‌ها امکان مدیریت، نظارت و دسترسی ایمن به منابع ارزشمند را می‌دهد. مثال‌ها ممکن است شامل فایل‌های الکترونیکی، سیستم‌های کامپیوتری، و منابع فیزیکی، مانند اتاق‌های سرور یا ساختمان‌ها باشد.

نگهداری مناسب و مراقبت مداوم مهم است. استفاده از امتیازدهی احتمال خطر در مدیریت هویت و دسترسی (IAM[1]) وضعیت امنیتی را افزایش می‌دهد. استفاده از یک مدل تخصیص احتمال خطر واضح، نظارت دقیق، و جداسازی صحیح رفتار آن می‌تواند به بررسی متقاطع سیستم‌های IAM کمک کند. دسترسی به هدف و فرکانس ردیابی برای امتیازدهی و نیز برای درک زمینه احتمال خطر حیاتی است.

۶-۲- رابط‌ها و API[2] های ناامن

محبوبیت استفاده از API همچنان در حال رشد است. ایمن‌سازی این رابط‌ها بسیار مهم شده است. APIها و ریزسرویس‌ها باید از نظر آسیب‌پذیری به دلیل پیکربندی نادرست، شیوه‌های ضعیف کدگذاری، عدم احراز هویت و مجوز نامناسب بررسی شوند. این نظارت‌ها به طور بالقوه می‌تواند رابط‌ها را در برابر فعالیت‌های مخرب آسیب‌پذیر کند.

نمونه‌های رایج عبارتند از:

۱. نقاط پایانی تایید نشده

۲. احراز هویت ضعیف

۳. مجوزهای بیش از حد

۴. کنترل‌های امنیتی استاندارد غیر فعال شده است

۵. سیستم‌های بدون رویه

۶. مسائل طراحی منطقی

۷. غیر فعال کردن ورود به سیستم یا نظارت

پیکربندی نادرست API ها و سایر رابط‌ها یکی از دلایل اصلی حوادث و نقض داده‌ها است. اینها می‌توانند به استخراج، حذف یا اصلاح منابع، تنظیمات داده‌ها یا وقفه در خدمات اجازه دهند.

سازمان‌ها به سرعت API ها (هم به عنوان ارائه دهندگان و هم به‌عنوان مصرف کنندگان) را از نظر اتصال و چابکی بهبود می‌بخشند. فعال کردن تجربیات دیجیتال برای توسعه‌دهندگان API و مشتریان توسعه‌دهندگان در مدیریت و ایمن سازی این API ها به دلیل رشد سریع و پذیرش آنها با یک وظیفه چالش برانگیز روبرو هستند.

۶-۳- پیکربندی نادرست و کنترل ناکافی تغییر

پیکربندی‌های نادرست، راه‌اندازی نادرست یا غیربهینه دارایی‌های محاسباتی است که ممکن است آن‌ها را در برابر آسیب‌های ناخواسته یا فعالیت‌های مخرب خارجی/داخلی آسیب‌پذیر کند. عدم دانش سیستم یا درک تنظیمات امنیتی و اهداف پلید می‌تواند منجر به پیکربندی اشتباه شود. برخی از تنظیمات اشتباه رایج عبارتند از:

۱. عناصر یا قالب ذخیره‌سازی داده‌های ناامن،

۲. مجوزهای بیش از حد

۳. اعتبار پیش فرض و تنظیمات پیکربندی بدون تغییر باقی می‌مانند

۴. کنترل‌های امنیتی استاندارد غیرفعال است

۵. سیستم‌های رویه نشده

۶. ورود به سیستم یا نظارت غیرفعال است

۷. دسترسی نامحدود به پورت‌ها و خدمات

۸. مدیریت اسرار ناامن

[1] Identity and Access Management
[2] Application Program Interface

۹. پیکربندی ضعیف یا عدم تأیید پیکربندی

پیکربندی نادرست منابع ابری یکی از دلایل اصلی نقض داده‌ها است و می‌تواند باعث حذف یا اصلاح منابع و وقفه‌های خدمت شود.

۶-۴- فقدان معماری و راهبرد امنیت ابری

راهبرد امنیت ابری و معماری امنیتی شامل: در نظر گرفتن و انتخاب مدل‌های استقرار ابر، مدل‌های خدمات ابری، ارائه‌دهندگان خدمات ابری (CSP)، در دسترس بودن منطقه خدمات، خدمات ابری خاص، اصول کلی است. راهبرد امنیت ابری به دو صورت می‌تواند باشد:

۱. طراحی آینده‌نگر IAM

۲. شبکه و کنترل امنیتی در حساب‌های ابری مختلف، فروشندگان، خدمت‌ها و محیط‌ها در محدوده هستند. در نظر گرفتن راهبرد باید مقدم بر طراحی باشد و آن را دیکته کند، اما معمول است که چالش‌های ابری نیازمند یک رویکرد تدریجی و به سرعت برای برنامه‌ریزی هستند. سرعت تغییر و رویکرد سلف خدمات رایج و غیرمتمرکز برای مدیریت زیرساخت ابری مانع از توانایی در نظر گرفتن ملاحظات فنی و تجاری و طراحی آگاهانه می‌شود.

با این حال، اگر می‌خواهیم تلاش‌های ابری موفق و ایمن باشند، ملاحظات و خطرات امنیتی را نباید نادیده گرفت. حکایت‌های موارد نقض صنعت نشان می‌دهد که فقدان چنین برنامه‌ریزی ممکن است منجر به شکست محیط‌های ابری و برنامه‌های کاربردی در برابر حملات سایبری یا انجام کارآمد آن شود. همین چالش‌ها می‌توانند به اجرای آسان‌تر راهبرد و طراحی امنیت ابری کمک کنند.

۶-۵- توسعه نرم‌افزار ناامن

نرم‌افزار پیچیده است و فناوری‌های ابری به پیچیدگی آن می افزایند در این پیچیدگی، عملکرد ناخواسته‌ای ظاهر می‌شود که می‌تواند امکان ایجاد و سوء استفاده کردن و تنظیمات نادرست احتمالی را فراهم کند. به لطف دسترسی به فضای ابری، عوامل تهدید می‌توانند از این «ویژگی‌ها» راحت تر از همیشه استفاده کنند.

CSP[1]ها (خط مشی امنیتی محتوا) ویژگی‌هایی را برای مدیریت هویت و دسترسی (IAM) ارائه می‌کنند که به توسعه‌دهندگان ابزارهای بررسی و راهنمایی در مورد اجرای صحیح را می‌دهد. این به نوبه خود نیاز به ساختن خدمات شرکت‌ها را از بین می‌برد که منابع را برای سرمایه‌گذاری در اولویت‌های تجاری مؤثرتر آزاد می‌کند.

اطمینان از درک هر یک از توسعه‌دهندگان از مسئولیت‌های مشترک شرکت با CSP نیازمند آموزش است. به‌عنوان مثال، اگر یک dayexploit-۰ برای Kubernetes گزارش شده باشد و یک شرکت از راه حل‌های Kubernetes CSP خود استفاده کند، CSP مسئولیت کاهش مشکل را بر عهده دارد. یک برنامه وب با استفاده از فناوری‌های بومی ابری با خطای سوء استفاده بر عهده توسعه‌دهنده است. در هر صورت، افشای اطلاعات حاصل بر شرکت تأثیر می‌گذارد.

هیچ توسعه دهنده‌ای قصد ایجاد نرم‌افزار ناامن را ندارد. با این حال، هر ماه رویه‌هایی توسط فروشندگان اصلی نرم‌افزار منتشر می‌شوند که خطاهایی را برطرف می‌کنند که می‌توانند برای تأثیرگذاری بر محرمانه بودن، یکپارچگی و یا در دسترس بودن یک سیستم استفاده شوند. همه خطاهای نرم‌افزار پیامدهای امنیتی ندارند، اما همانطور که تاریخ ثابت کرده است، می‌توانند به تهدیدهای مهمی تبدیل شوند. استقبال از فناوری‌های ابری به شرکت‌ها این امکان را می‌دهد که تمرکز خود را بر روی چیزی که مختص کسب وکارشان است متمرکز کنند، در حالی که به CSP اجازه می‌دهند هر چیز دیگری را که ممکن است کالایی شود، مدیریت کند.

۶- ۶- منابع شخص ثالث ناامن

در دنیایی که پذیرش رایانش ابری به سرعت در حال افزایش است، یک منبع شخص ثالث می‌تواند معانی متفاوتی داشته باشد: از کد منبع باز، از طریق محصولات SaaS و خطرات API (مسئله امنیتی)، و تا یک خدمت مدیریت شده که توسط یک فروشنده ابری ارائه می‌شود. خطرات ناشی از منابع شخص ثالث نیز آسیب‌پذیری‌های زنجیره تامین محسوب می‌شوند زیرا بخشی از فرآیند ارائه محصولات یا خدمات شما هستند. این خطرات در هر محصول و خدمات مصرف شده وجود دارد. با این حال، به دلیل اتکای فزاینده به خدمات شخص ثالث و محصولات مبتنی بر نرم‌افزار در سال‌های اخیر، سوء استفاده‌های بیشتری از این آسیب‌پذیری‌ها و پیکربندی‌های قابل هک رخ می‌دهد. در واقع، طبق تحقیقات دانشگاه ایالتی کلرادو، دو سوم نقض‌ها ناشی از آسیب‌پذیری‌های تامین‌کننده یا شخص ثالث است.

از آنجایی که یک محصول یا خدمات مجموعه‌ای از تمام محصولات و خدمات دیگری است که استفاده می‌کنند، سوء استفاده می‌تواند در هر نقطه‌ای از زنجیره شروع شود و از آنجا زیاد شود. برای هکرهای مخرب، این بدان معنی است که برای

[1]Content Security Policy

رسیدن به هدف خود، آنها "فقط" باید به‌دنبال ضعیف‌ترین پیوندها به‌عنوان یک نقطه ورود باشند. در دنیای نرم‌افزار، استفاده از SaaS و منبع باز برای مقیاس‌پذیری یک روش معمول است. هکرهای مخرب فرصت یکسانی برای رشد دریافت می‌کنند و با بهره‌برداری مشابه به اهداف بیشتری آسیب می‌رسانند.

۶-۷- آسیب‌پذیری‌های سیستم

آسیب‌پذیری‌های سیستم نقص در پلت‌فرم‌های خدمات ابری هستند. آنها ممکن است در تلاشی برای به خطر انداختن محرمانه‌بودن، یکپارچگی و در دسترس بودن داده‌ها مورد سوء استفاده قرار گیرند و به طور بالقوه عملیات سروی را مختل کنند. همه مؤلفه‌ها می‌توانند دارای آسیب‌پذیری‌هایی باشند که ممکن است خدمات ابری را در معرض حمله قرار دهند. اجرای شیوه‌های سخت‌سازی امنیتی که با دسته‌های آسیب‌پذیری زیر هم‌سو هستند برای کاهش خطرات امنیتی آنها ضروری است. چهار دسته اصلی از آسیب پذیری‌های سیستم وجود دارد:

❖ **آسیب‌پذیری‌های جدید**

آسیب‌پذیری‌های تازه کشف‌شده که رویه‌هایی برای آن‌ها وجود ندارد. هکرها به سرعت برای سوء استفاده از آسیب‌پذیری‌هایی اقدام می‌کنند، زیرا تا زمانی که رویه‌ها نصب نشده باشند، هیچ چیزی برای متوقف کردن آنها وجود ندارد.

❖ **رویه‌های امنیتی از دست رفته است**

هنگامی که رویه‌های آسیب‌پذیری‌های حیاتی شناخته شده در دسترس قرار می گیرند، استقرار آنها در اسرع وقت سطح حمله سیستم را کاهش می‌دهد. با گذشت زمان، آسیب‌پذیری‌های جدیدتر سیستم کشف شده و رویه‌ها در دسترس قرار خواهند گرفت.

❖ **آسیب‌پذیری‌های مبتنی بر پیکربندی**

این نوع آسیب‌پذیری زمانی ایجاد می‌شود که یک سیستم با تنظیمات پیش‌فرض یا پیکربندی نادرست مستقر شود.

❖ **اعتبارنامه‌های ضعیف یا پیش‌فرض**

فقدان اعتبارنامه‌های احراز هویت قوی، دسترسی آسان مهاجمان بالقوه به منابع سیستم و داده‌های مرتبط را فراهم می‌کند.

۶-۸- افشای تصادفی داده‌های ابری

خدمات‌های ابری شرکت‌ها را قادر می‌سازند تا با سرعتی که قبلاً دیده نشده بود، نوآوری و مقیاس کنند. با این حال، پیچیدگی ابر و تغییر مالکیت خدمات ابری، با تیم‌ها و واحدهای تجاری متنوع، اغلب منجر به فقدان حاکمیت و کنترل امنیتی می‌شود. افزایش تعداد پیکربندی‌ها برای منابع ابری در CSPهای مختلف، پیکربندی‌های نادرست را رایج‌تر می‌کند. شفافیت موجودی ابر و قرار گرفتن در معرض شبکه کافی می‌تواند منجر به نشت ناخواسته داده شود.

قرار گرفتن در معرض نشت‌داده‌ها هنوز هم گسترده است. بیش از ۵۵ درصد از شرکت‌ها حداقل یک پایگاه داده دارند که در حال حاضر به صورت عمومی در معرض اینترنت است. بسیاری از این پایگاه‌های اطلاعاتی از رمزهای عبور ضعیف استفاده می‌کنند یا نیازی به احراز هویت ندارند، که آنها را به هدفی آسان برای مهاجمان تبدیل می‌کند که به طور مداوم اینترنت را در جستجوی چنین پایگاه‌های اطلاعاتی در معرض جستجو اسکن می‌کنند.

با توجه به اینکه یک سرور Elastic search ناامن می‌تواند در عرض هشت ساعت نفوذ کند، چنین نفوذها باید در اسرع وقت اصلاح شوند.

۶-۹- پیکربندی نادرست و بهره‌برداری از بارهای کاری بدون سرور و محفظه

مهاجرت به زیرساخت‌های ابری و اتخاذ شیوه‌های DevOps به تیم‌های فناوری اطلاعات این امکان را می‌دهد که سریع‌تر از همیشه بهره‌وری را به کسب‌وکار ارائه کنند. مدیریت و مقیاس‌بندی زیرساخت‌ها و کنترل‌های امنیتی برای اجرای برنامه‌ها همچنان بار مهمی بر دوش تیم‌های توسعه است تیم‌های زیرساخت قدیمی که برای مدیریت محیط‌های اولیه استفاده می‌شوند باید مهارت‌های جدیدی مانند Infrastructureas Code و امنیت ابری را بیاموزند.

همین تیم‌ها باید مسئولیت بیشتری در قبال شبکه و کنترل‌های امنیتی که از برنامه‌هایشان پشتیبانی می‌کند، بپذیرند. بارهای کاری محفظه‌ای بدون سرور و ابری می‌توانند مانند یک گلوله نقره‌ای برای این مشکل به نظر برسند و این مسئولیت را بر عهده ارائه‌دهنده خدمات ابری (CSP) می‌گذارند. با این حال، به سطح بالاتری از بلوغ امنیت ابر و برنامه نسبت به مهاجرت ماشین‌های مجازی به ابر نیاز دارد.

در یک مدل بدون سرور، CSP مسئولیت امنیت و مدیریت زیرساخت های اساسی را بر عهده می‌گیرد. علاوه بر مزایای توسعه و عملیاتی، این امر سطح حمله را کاهش می‌دهد زیرا CSPها به طور پیش فرض کد تابع را در محفظه‌های کوتاه مدت اجرا می‌کنند. سیستمی که دائماً تازه می‌شود، به طور قابل توجهی ماندگاری را در صورت کدهای مخرب محدود می‌کند. با

این حال، اگر یک CSP به مشتریان اجازه دهد تا محفظه‌های بدون سرور را با طول عمر بیشتر و تنظیمات "شروع گرم" پیکربندی کنند، محیط از امنیت کمتری برخوردار می‌شود. خطرات اضافی شامل سیستم فایل موقت و حافظه مشترک نیز ممکن است اطلاعات حساس را درز کند. دسترسی به حافظه موقت ممکن است برای میزبانی یا اجرای بدافزار استفاده شود و باید با کد برنامه پاک شود.

۶-۱۰- جرایم سازمان یافته / هکرها

تهدیدهای پایدار پیشرفته (APTs) یک اصطلاح گسترده برای توصیف کمپین حمله‌ای است که در آن یک مهاجم یا تیمی از متجاوزان، حضور غیرقانونی و طولانی مدت در یک شبکه برای استخراج داده‌های بسیار حساس ایجاد می‌کنند. این تیم‌ها ممکن است شامل دولت‌های ملی و همچنین باندهای جنایتکار سازمان‌یافته باشند. اصطلاح جرایم سازمان‌یافته به معنای ابزاری برای توصیف روشی است که در آن سطح سازمانی یک گروه در هنگام ایجاد اعمال برنامه‌ریزی‌شده و منطقی که بازتاب تلاش‌های افراد گروه است، خواهد داشت. APT[1] ها ترفندها و پروتکل‌های پیچیده‌ای برای نفوذ به اهداف خود ایجاد کرده‌اند. غیرمعمول نیست که گروه‌های APT ماه‌ها را بدون شناسایی در یک شبکه هدف سپری کنند. این زمان طولانی به آنها اجازه می‌دهد تا به سمت داده‌ها یا دارایی‌های تجاری بسیار حساس حرکت کنند. برخی از گروه‌های APT از لحاظ تاریخی نیز صنایع یا سازمان‌های خاصی را زیر نظر داشتند.

جامعه اطلاعاتی تهدیدات را از گروه‌های APT مطالعه می‌کند. گزارش‌های اطلاعاتی تهدید مربوط به سازمان‌ها و دولت‌ها را درباره گروه‌های APT و رفتار آنها آموزش می‌دهد. سازمان‌ها می‌توانند با انجام تمرین‌های تیمی برای شبیه‌سازی رفتار گروه‌های APT که در گزارش‌ها شرح داده شده‌اند، بهتر از خود محافظت کنند. چنین تمرین‌های سایبری به سازمان‌ها اجازه می‌دهد تا قابلیت‌های تشخیص سایبری خود را در برابر TTP[2]های مختلف مرتبط با گروه‌های APT آزمایش و بهبود بخشند. سازمان‌ها همچنین باید فعالیت‌های شکار تهدید را برای شناسایی حضور APT ها در شبکه‌های خود انجام دهند.

۶-۱۱- استخراج داده‌های ذخیره‌سازی ابری

استخراج داده‌های ذخیره‌سازی ابری رویدادی است که شامل اطلاعات حساس، محافظت شده یا محرمانه است. این داده‌ها ممکن است توسط فردی خارج از محیط عملیاتی سازمان منتشر، مشاهده، سرقت یا استفاده شود. استخراج داده‌ها ممکن است هدف اصلی یک حمله هدفمند باشد و ممکن است ناشی از یک آسیب پذیری یا پیکربندی نادرست، آسیب‌پذیری‌های برنامه یا عملکرد ضعیف امنیتی باشد.

نفوذ ممکن است شامل هر نوع اطلاعاتی باشد که برای انتشار عمومی در نظر گرفته نشده است، به عنوان مثال، اطلاعات سلامت شخصی، اطلاعات مالی، اطلاعات قابل شناسایی شخصی (PII[3])، اسرار تجاری، و مالکیت معنوی.

از آنجایی که داده‌ها یک دارایی اصلی هستند، سهولت استفاده، پیکربندی، کشش، انعطاف‌پذیری و چندین خدمت مناسب برای همه نیازهای منطقی، ذخیره‌سازی داده‌های ابری را بسیار جذاب می‌کند. مکان‌های متعددی برای استخراج آن وجود دارد. این می‌تواند به دلیل خطاهای انسانی یا سوء استفاده باشد، مانند پیکربندی نادرست یک خدمت PaaS. اشیاء ذخیره‌سازی همچنین ممکن است داده‌ها یا فایل‌هایی را که به صورت خارجی از طریق برنامه‌های ذخیره‌سازی ابری شخصی به اشتراک گذاشته می‌شوند، در معرض نمایش قرار دهند.

۷- انواع حملات به ابر

انواع حملاتی که می‌تواند به ابر انجام بپذیرد و تهدیدی بر این فناوری باشد و همچنین راهکارهای مقابله با این حملات عبارتند از[۷]:

۷-۱- حمله سیل

در حمله سیل، دشمن به راحتی می‌تواند داده‌های جعلی ایجاد کند و هر زمان که سرور بیش از حد بارگذاری می‌شود، کار را به نزدیک‌ترین سرور اختصاص می‌دهد و سرور خاص خود تخلیه می‌شود. در حین تخصیص، درخواست پردازش توانمندتر و سریعتر را ارائه می‌دهد. در واقع یک نوع حمله انکار خدمت است که زمانی رخ می‌دهد که تعداد زیادی ترافیک درخواست خدمات وجود داشته باشد. این حمله باعث می‌شود سرور یا میزبان به سبب بارگذاری بیش از حد اطلاعات در حافظه سیستم، دچار اختلال گردد.

در حمله سیل Ping[4]، تمرکز مهاجم بر پهنای باند شبکه است. در واقع مهاجمان در تلاش هستند تا با تمرکز بر روی شبکه، پهنای باند بتوانند نفوذ کنند، یک شبکه با بسته‌های

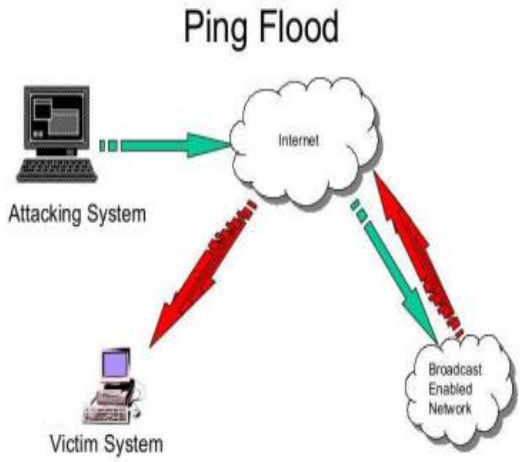
[1] Advanced Persistent Threats
[2] Tactics, Techniques and Procedures
[3] Personally Identifiable Information
[4] Packet Internet Groper

درخواست انعکاس ICMP[1] پر می‌شود تا ترافیک قانونی عبور از شبکه را کند یا متوقف کند. در شکل (۴) نشان داده شده است[۱۳].

در واقع حملات سیل زمانی اتفاق می‌افتند که سیستم ترافیک زیادی را برای محدود کردن سرور دریافت می‌کند و باعث کاهش سرعت و در نهایت توقف آن می‌شود[۱۵].

به طور کلی، یک حمله شامل افزایش شدید ترافیک شبکه با تعداد زیادی پیام نادرست یا غیر ضروری است. یکی از رایج‌ترین حملات، سیل یا Ping شیوه پیام کنترل اینترنت (ICMP) است[۱۵].

این حمله سیل ICMP (Ping) متمرکز است، زیرا به اتصالات شبکه دستگاه مورد نظر به‌صورت جعلی غلبه می‌کند و باعث می‌شود از دریافت درخواست‌های قانونی جلوگیری شود[۱۵].



شکل (۴): حمله سیل [۷]

- **راه‌حل حمله سیل**

استفاده از فن ارسال پیام جهت جلوگیری از برقراری ارتباط همه سرورها با یکدیگر، از حمله سیلابی جلوگیری می‌کند.

۷-۲- حمله به کانال جانبی

با قرار دادن یک ماشین مجازی مخرب در نزدیکی یک سرور ابری، مورد هدف حمله قرار می‌گیرد، با این روش یک حمله کانال جانبی ایجاد می‌شود. در واقع این یک سوء استفاده امنیتی است که هنگام انجام عملیات رمزنگاری و مهندسی معکوس انجام می‌شود و جزئیات رمزنگاری ماشین هنگام جمع‌آوری اطلاعات در مورد کل ماشین میزبان اتفاق می‌افتد.

انواع حمله کانال جانبی عبارتند از:

۱. حمله رمزنگاری آکوستیک

این قطعه می‌تواند انتشار مدارهای الکترونیکی را در زمانی که کاربر از رایانه استفاده می‌کند نظارت کند. همچنین می‌تواند اطلاعاتی در مورد مصرف برق و میدان‌های الکترومغناطیسی ارسال شده توسط دستگاه جمع‌آوری کند.

۲. حمله کش

در یک محیط سیستم فیزیکی، حملات کش از زمان و نحوه پردازش کش بهره‌برداری می‌کند.

۳. حمله تجزیه و تحلیل خطا

این نوع حملات که هنگام بروز خطا در هنگام محاسبه سیستم، اطلاعات را از یک سیستم جمع‌آوری می‌کند.

۴. حمله زمان‌بندی

نوعی از حمله است که حرکت داده‌ها را در CPU[2] و حافظه ردیابی می‌کند.

۵. راه‌حل حمله کانال جانبی

دستگاه دیواره‌آتش مجازی طبق شکل(۵) با رمزگشایی و رمزگذاری تصادفی ترکیب شده است تا بتواند به امنیت در برابر حمله کانال جانبی دست یابد. این ترکیب امنیت را هم از قسمت جلویی و هم در انتهای معماری محاسبات ابری فراهم می‌کند.

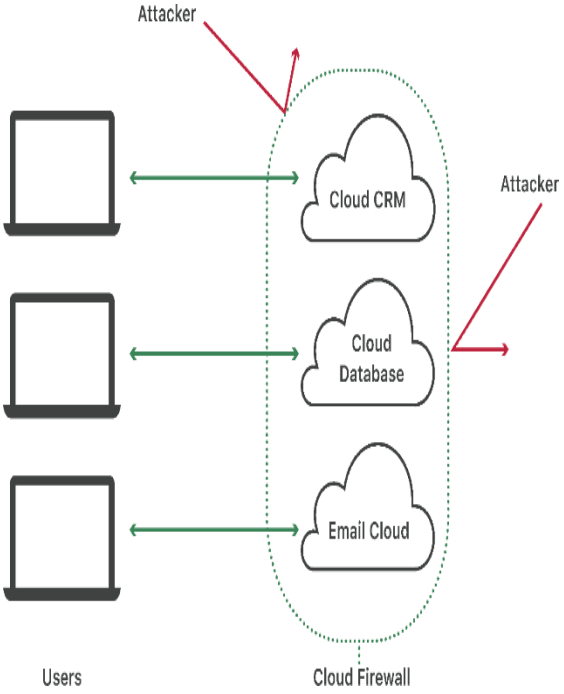
دیواره‌آتش ابری یک محصول امنیتی است که مانند دیواره‌آتش سنتی، ترافیک شبکه بالقوه مخرب را فیلتر می‌کند. برخلاف دیواره‌های‌آتش سنتی، دیواره‌های‌آتش ابری در فضای ابری میزبانی می‌شوند. این مدل ارائه شده توسط ابر برای دیواره‌های‌آتش، فایروال به عنوان سرویس (FWaaS[3]) نیز نامیده می‌شود[۱۹].

دیواره‌های‌آتش مبتنی بر ابر یک مانع مجازی در اطراف پلتفرم‌ها، زیرساخت‌ها و برنامه‌های کاربردی ابری تشکیل می‌دهند، همانطور که دیواره‌های‌آتش سنتی مانعی در اطراف

[1] internet control message protocol

[2] Central Procesing Unite
[3] Firewall as a service

شبکه داخلی سازمان می‌سازند. دیواره‌های‌آتش ابری همچنین می توانند از زیرساخت‌های داخلی محافظت کنند[۱۹].

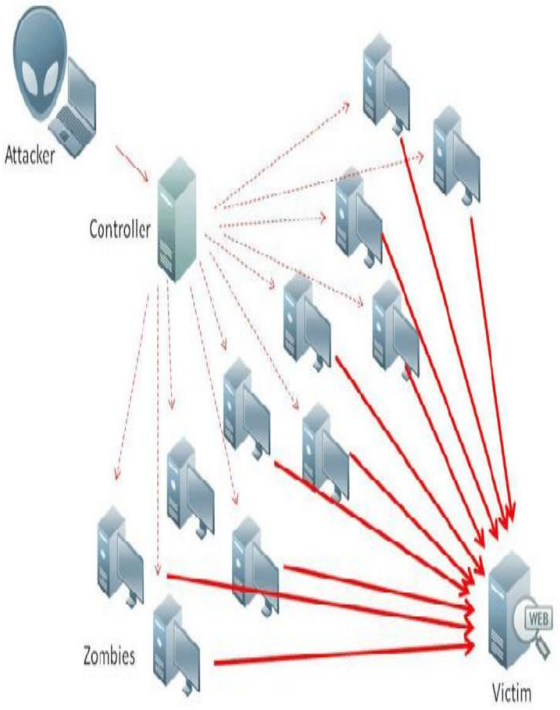


شکل(۵): دیواره آتش [۱۹]

۷-۳- حمله تزریق بدافزار

در حمله تزریق بدافزار، طبق شکل (۶) برخی از کدها یا خدمات‌هایی که قبلاً در فضای ابری اجرا شده‌اند، توسط مهاجم به کد یا سرویس مخرب تبدیل می‌شوند. این نوع حمله خارجی به عنوان حمله جعل داده نیز شناخته می‌شود. در این حمله مهاجم داده‌ها را از اینترنت می‌دزد و به جای آن داده‌های مخرب را در اختیار کاربران نهایی قرار می‌دهد تا به طور غریزی و بدون اطلاع کاربر، اطلاعات بیهوده را بارگذاری کنند. این یکی از حملات مهمی است که اجرای سرویس مخرب را به ابر تزریق می‌کند.

در این حمله، دشمن مدل اجرای سرویس مخرب خود (SaaS یا PaaS) یا نمونه ماشین مجازی (IaaS) خود را ایجاد می‌کند و آن را به سیستم Cloud اضافه می‌کند. سپس، حریف باید به سیستم ابری وانمود کند که برخی از نمونه‌های اجرای خدمت جدید و در میان نمونه‌های معتبر برای خدمت خاصی است که توسط دشمن مورد حمله قرار گرفته است. در صورت موفقیت آمیز بودن این اقدام، Cloud به طور خودکار درخواست‌های کاربر معتبر را به اجرای سرویس مخرب هدایت می کند و کد دشمنان اجرا می‌شود. سناریوی اصلی در پس حمله تزریق بدافزار ابری این است که مهاجم یک نسخه دستکاری شده/اشتباه از نمونه سرویس قربانیان را منتقل می کند تا نمونه مخرب بتواند به درخواست‌های سرویس قربانیان دسترسی پیدا کند. برای دستیابی به این هدف، مهاجم باید کنترل داده‌های قربانیان را در فضای ابری به دست آورد[۱۴].



شکل(۶): حمله تزریق بدافزار [۷]

- **راه‌حل‌های حمله تزریق بدافزار**

۱. ایجاد یک حساب کاربری و ذخیره همان تصویر در یک محیط ذخیره‌سازی تصویر ابری از بهره برداری از این فرآیند جلوگیری می‌کند. همین تصویر را می‌توان با استفاده از جدول تخصیص فایل بررسی و احراز هویت کرد.

۲. اقدام متقابل دیگر ذخیره نوعی سیستم عامل حساب در زمانی که مشتری سعی می‌کند آن را باز کند. این روش با ایجاد یک رویه بررسی متقاطع کار می‌کند که O.Stype دارندگان حساب را در مقابل نوع سیستم عامل مشتری بررسی می‌کند.

هنگامی که یک کاربر جدید با یک حساب ابری شروع به کار می‌کند، فروشنده ابری برای شناسایی کاربر به طور خودکار تصویری از سیستم مجازی کاربر در مخزن ابر ایجاد می‌کند.

۷-۴- حمله احراز هویت

حمله احراز هویت یک مشکل نرم و هدفمند در پلت‌فرم خدمات مجازی است. راه‌های زیادی برای احراز هویت یک کاربر خاص در پلت‌فرم محاسبات ابری با بدون اطلاع از دانش کاربر وجود دارد. با ایمن کردن فرآیند احراز هویت، تمرکز اصلی مهاجم هدف قرار دادن سازوکار و روش‌های آن است. معماری IaaS مناسب‌ترین پلتفرم غیر از SaaS و PaaS برای ارتباطات داده ایمن خواهد بود.

- **راه‌حل برای حمله احراز هویت**

فن‌های اصلی احراز هویت به سازوکار نام کاربری و رمز عبور برای ایمن کردن حساب وب یا حساب کاربری بستگی دارد، به جز برخی از سایت‌های مالی و وب سایت‌های بانکی از روش‌های دیگری مانند احراز هویت دو مرحله‌ای، رمز عبور مشترک، صفحه‌کلید مجازی و غیره استفاده می‌کنند.

۷-۵- جدول مقایسه حملات و تجزیه‌وتحلیل بین حملات :

با بررسی حملاتی که می‌تواند در رایانش ابری انجام بگیرد به طور مختصر توضیح داده شد جدول (۴) این حملات را مورد مقایسه قرار داده میزان آسیب‌پذیری و نوع حمله و عواقب آنها را بیان می‌کند.

جدول (۴): انواع مختلف حملات مقایسه و تجزیه و تحلیل [۷]

حمله ها	نوع حمله	دلیل آسیب پذیری	نقض امنیتی	عواقب
حمله انکار سرویس	حمله خارجی/داخلی	آسیب پذیری ذخیره سازی آسیب پذیری های مرکز داده	مسائل امنیتی سطح مجازی سازی	وقفه و اصلاح نرم افزار یدون نیاز یه پاسخگویی یه خدمات قانونی
حمله تزریق ید افزار	حمله خارجی	از دست دادن قدرت و کنترل محیطی	مسائل امنیتی سطح فیزیکی	تغییر سخت افزار و سرقت
حمله سیل	حمله خارجی/داخلی	آسیب‌پذیری مسیر یا داده‌ها	مسائل امنیتی سطح جریان تراقیک و همچنین مسائل ارتباطی	ازدحام تراقیک شیکه یدون اتصال بیشتر و در نتیجه حمله‌dos
حمله کانال جانبی	حمله غیرفعال/فعال	آسیب پذیری سیستم عامل	استفاده از vm مخرب برای حمله یه ایر	یر پلتفرم سخت افزاری و نرم افزاری تاثیر خواهد گذاشت
حمله احراز هویت	حمله خارجی/داخلی	آسیب پذیری داده های کاربر آسیب پذیری دسترسی	نقض داده ها ربودن حساب ها	دسترسی غیرمجاز مشکلات کاربر قانونی است

۸- روش‌های حفاظت در رایانش ابری

شرکت‌های رایانش ابری از ویژگی‌های امنیتی متنوعی برای ایمن‌سازی اطلاعات و داده‌ها در فضای ابری استفاده می‌کنند برخی از این ویژگی‌های مورد استفاده شامل دیواره آتش، سیستم‌های تشخیص نفوذ با اطلاعات ورود به سیستم، رمزگذاری داده‌ها، استفاده از امنیت فیزیکی مؤثر و محافظت از برنامه‌ها و نرم‌افزارهای مستقل دربرابر حملات خارجی است[۸].

بعد از شناخت حملات و چالش‌ها و مسائل امنیتی در ابر باید راه‌های مقابله با این تهدیدات را مورد بررسی قرار دهیم و شامل فناوری‌ها، کنترل‌ها، فرآیندها و سیاست‌هایی است که برای محافظت از سیستم‌ها، داده‌ها و زیر ساخت‌های مبتنی بر ابر کاربر ترکیب می‌شوند. این یک زیر دامنه از امنیت کامپیوتر و به طور گسترده‌تر، امنیت اطلاعات است.

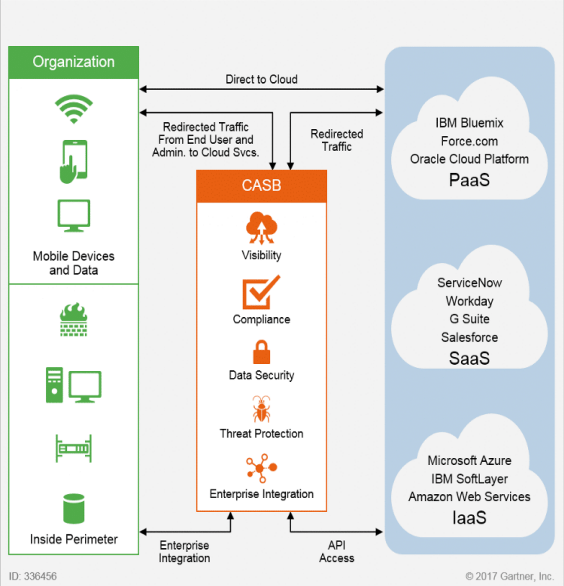
این یک مسئولیت مشترک بین کاربر و ارائه دهنده خدمات ابری است. کاربر یک راهبرد امنیت ابری را برای محافظت از داده‌های خود، رعایت مقررات نظارتی و محافظت از حریم خصوصی مشتریان خود اجرا می‌کند. که به نوبه خود کاربر را از پیامدهای اعتباری، مالی و قانونی نقض داده‌ها و از دست دادن داده‌ها محافظت می‌کند. در ادامه با نمونه‌ای از روش‌های حفاظت در ابر را معرفی می‌کنیم [۶] و [۱۶].

۸-۱- کارگزار امنیت ابر

کارگزار امنیت ابر طبق شکل (۷) که به اختصار CASB[1] نامیده می‌شود، نرم‌افزاری است که بین، مصرف‌کننده خدمات ابری و ارائه دهنده(های) خدمات ابری قرار می‌گیرد. یک CASB کنترل‌های امنیتی شما را از زیر ساخت‌های داخلی به فضای ابری گسترش می‌دهد. کمک به اجرای سیاست‌های امنیتی، انطباق و حاکمیت برای برنامه‌های ابری شما معمولاً در محل قرار می‌گیرد یا در فضای ابری میزبانی می‌شود.

یک CASB به شما کمک می‌کند در برابر خطرات امنیت ابری سطح بالا دفاع کنید و از نظارت مداوم و کاهش رویدادهای پرخطر پشتیبانی کنید. این کار را با ایمن کردن اطلاعات در حال حرکت بین محیط داخلی و فضای ابری با استفاده از سیاست‌های امنیتی سازمان شما انجام می‌دهد.

[1] Cloud Access Security Broker



شکل (۷): مدل کارگزار امنیتی Cloud Access [۱۶]

یک CASB از شما در برابر حملات سایبری با جلوگیری از بدافزار محافظت می‌کند و داده‌های شما را با استفاده از رمزگذاری انتها به انتها ایمن می‌کند که از رمزگشایی محتوا توسط کاربران خارجی جلوگیری می‌کند.

۸-۲- اتحاد امنیت ابر

اتحاد امنیت ابر[1] یک سازمان غیرانتفاعی است که به توسعه و افزایش آگاهی از بهترین شیوه‌ها برای حفظ یک محیط محاسبات ابری ایمن اختصاص دارد.

این یک سازمان است که راهنمایی‌های امنیتی ویژه صنعت ابر را در قالب آموزش، تحقیق، رویدادها و محصولات ارائه می‌دهد. این رهنمود مستقیماً از تخصص موضوعی ترکیبی متخصصان صنعت، انجمن‌ها، دولت‌ها و اعضای فردی و شرکتی CSA استفاده می‌شود.

۸-۳- محافظت از آسیب‌پذیری

ارائه‌دهنده خدمات ابری باید مدیریت رویه را بهبود بخشد. آنها باید آسیب‌پذیری خدمات ابری خود را مرتباً بررسی کنند و همیشه ابر را به‌روزرسانی و نگهداری کنند تا نقطه دسترسی احتمالی را محدود کرده و خطر حمله هکرها به ابر را کاهش دهند. ارائه‌دهنده خدمات ابری همچنین ممکن است از سیستم تشخیص نفوذ (IDS[2]) استفاده کند تا مطمئن شود که خدمات ابری ارائه شده ایمن است.

۸-۴- مدیریت شناسایی و احراز هویت

هنگامی که کاربران می‌خواهند به داده‌های ذخیره شده در فضای ابری دسترسی داشته باشند، نه تنها با استفاده از نام کاربری و رمز عبور بلکه باید از داده‌های دیجیتالی نیز احراز هویت شوند. فن احراز هویت چند سطحی معرفی شده می‌تواند در محاسبات ابری نیز پیاده‌سازی شود. این فن قبل از اینکه کاربر بتواند به خدمات ابری دسترسی پیدا کند، رمز عبور را در چندین سطح ایجاد می‌کند. احراز هویت ناشناس (یعنی هویت کاربر از ابر محافظت می‌شود) همچنین می‌تواند در جایی اجرا شود که فقط کاربران معتبر قادر به رمزگشایی اطلاعات هستند. طرح احراز هویت رمز عبور جدید می‌تواند به منظور بهبود امنیت خدمت‌های ابری مورد استفاده قرار گیرد.

برای احراز هویت کاربر، ابتدا توسط شخص ثالث و سپس توسط مالک داده احراز هویت دو مرحله‌ای انجام می‌شود. مالک داده فهرستی از کاربران مجاز را همراه با شناسه ورود و رمز عبور به شخص ثالث می‌دهد. شخص ثالث یک پایگاه داده برای اعتبارسنجی کاربر می‌سازد. زمانی که کاربر با شناسه کاربری و رمز عبور وارد پایگاه داده می‌شود، شخص ثالث کاربر را با بررسی پایگاه داده خود تصدیق می‌کند. اگر کاربر مجاز باشد، شخص ثالث کلید محرمانه را بدون کد عبور، صادرکرده و مالک داده را نیز باخبر می‌سازد[۱۲].

۸-۵- ارائه دهنده خدمات ابری تایید شده

کاربر باید مطمئن شود که ارائه دهنده خدمات ابری مناسب را کشف کرده است. هر ارائه دهنده خدمات ابری رویکردهای متنوعی در زمینه مدیریت داده در فضای ابری دارد. ارائه دهنده خدمات ابری با سابقه و با تجربه، قابل اعتمادتر و انتخاب بهتری است. علاوه بر این، استانداردها و مقررات ارائه دهنده خدمات ابری نیز بسیار مهم هستند. نمونه‌هایی از ارائه دهندگان خدمات ابری تایید شده عبارتند از: گوگل و مایکروسافت، خدمات وب آمازون (AWS[3]) و IBM[4].

[1] Cloud Security Alliance (CSA)

[2] Intrusion Detection System
[3] Amazon Web Services
[4] International Business Machines

۸-۶- از خدمات ابری هوشمندانه استفاده کنید

داده‌های ذخیره شده در ابر باید محرمانه باشد و حتی ارائه دهنده خدمات ابری نباید به آن اطلاعات دسترسی داشته باشد. داده‌های ذخیره شده در ابر باید به خوبی رمزگذاری شوند تا از امنیت اطلاعات کاربران اطمینان حاصل شود. هرکسی که نیاز به دسترسی به داده‌های موجود در فضای ابری دارد باید قبل از انجام این کار از کاربران اجازه بگیرد.

۸-۷- امکانات برای بازیابی

ارائه‌دهنده خدمات ابری باید مسئولیت بازیابی اطلاعات کاربران را در صورت از دست رفتن داده‌ها به دلیل مشکلات خاص بر عهده بگیرد. ارائه‌دهنده خدمات ابری باید اطمینان حاصل کند که پشتیبان‌گیری مناسبی دارد و می‌تواند داده‌های محرمانه کاربران را بازیابی کند که ممکن است پرهزینه باشد.

۸-۸- زیرساخت‌های سازمانی

کاربر باید داده‌هایی را که می خواهد در زیرساخت ابری نگه دارد، ایمن کند. ارائه‌دهنده خدمات ابری باید زیرساختی را فراهم کند که کاربران را برای نصب و پیکربندی اجزای سخت‌افزاری مانند دیواره‌های آتش، روترها، سرور و سرور پروکسی تسهیل کند.

۸-۹- کنترل دسترسی

ارائه‌دهنده خدمات ابری باید کنترل دسترسی به داده‌ها را با حقوق تنظیم کند و کاربرانی که به داده‌ها دسترسی دارند باید هر بار توسط ارائه‌دهنده خدمات ابری تأیید شوند. ارائه‌دهنده خدمات ابری باید اطمینان حاصل کند که فقط کاربران مجاز می‌توانند به داده‌های ذخیره‌شده در ابر دسترسی داشته باشند. این روش می‌تواند به کاهش خطر دسترسی به داده‌ها توسط کاربران غیرمجاز کمک کند و بنابراین یک محیط امن بسیار برای ذخیره داده‌های حساس فراهم می‌کند. علاوه بر این، حسابرسی شخص ثالث نیز می‌تواند یکی از گزینه‌های جایگزین برای اطمینان از یکپارچگی داده‌های ذخیره‌سازی در ابر باشد. با این حال، مسیر عملیات حسابرسی باید دارای ویژگی‌های زیر باشد:

- **محرمانه‌بودن / رازداری:** پروتکل‌های حسابرسی باید اطلاعات کاربر را در برابر حسابرس محرمانه نگه دارد.
- **ممیزی پویا:** پروتکل حسابرسی باید تجدید داده‌ها را در فضای ابری حفظ کند.
- **حسابرسی دسته‌ای:** پروتکل حسابرسی باید حسابرسی دسته‌ای را برای کاربران چندگانه و ابرها حفظ کند.

۸-۱۰- رویدادهای بررسی امنیتی

کاربران باید قرارداد روشنی با ارائه‌دهنده خدمات ابری داشته باشند تا در صورت بروز هرگونه حادثه یا نقض داده‌ها/اطلاعات حساس ذخیره شده در ابر، کاربران بتوانند ادعا کنند. کاربران باید قبل از استفاده از خدمات‌های ابری ارائه شده توسط آن ارائه دهنده خدمات ابری خاص، با ارائه دهنده خدمات ابری توافق داشته باشند. کاربران باید اطمینان حاصل کنند که ارائه دهنده خدمات ابری جزئیات کافی در مورد اجرای ضمانت‌ها، اصلاح خرابی و احتمال گزارش‌دهی ارائه می‌دهد.

۸-۱۱- مقررات ذخیره‌سازی داده‌ها

معماری محیط ابری یک جنبه مهم برای تضمین امنیت داده های ذخیره شده در ابر است. کاربران باید مفهوم مقررات ذخیره‌سازی داده را که ارائه دهنده خدمات ابری از آن پیروی می‌کند، درک کنند. ارائه دهنده خدمات ابری که راه‌حل‌های امنیتی منطبق با مقرراتی مانند قوانین HIPAA، PCI DSS و قوانین حفاظت از داده اتحادیه اروپا ارائه می‌کند، بهترین انتخاب هستند.

۹- نتیجه گیری

با توسعه فناوری در دنیا و حرکت سازمان‌ها به سمت پیشرفت، نوآوری، سرعت و دقت نیاز به فناوری جدید داشتند و با به وجود آمدن رایانش ابری این خدمات در اختیار سازمان‌ها و کاربران قرار گرفت ما در این مقاله سعی کردیم مسائل امنیتی ای که خاص ابر می‌باشد و همچنین چالش‌ها و نگرانی‌های جدیدی که در این فناوری اطلاعات و داده‌های کاربران و سازمان‌ها که می خواهند از این فناوری استفاده کنند را تا حد امکان بیان کنیم و راهکارهای هم را نسبت به مقابله با آنها را ارائه دهیم.

۱۰- مراجع

[1] A. Bahadur and A. Sadeghi, "Security in cloud computing based on network security based on intelligent methods," Applied Science Studies in Engineering, pp. 65-74, 2019.

[2] N. Mansoori and B. Mohammad Hassanizadeh, and R. Ghafari "Security-based work scheduling algorithm using particle swarm optimization technique and multiple adaptive learning to improve security in cloud computing environment" Electronic and Cyber Defense 159-178 pp, 2019.

[3] J. Michael Brook, A .Stone Getsin, and M. Roza, “Top Threats to Cloud Computing”2022
[4]I. Kanwal, H. Shafi, S. Memon, and M. H. Shah, "Cloud computing security challenges: A review," in Cybersecurity, Privacy and Freedom Protection in the Connected World: Proceedings of the 13th International Conference on Global Security, Safety and Sustainability, London, pp. 459-469, Springer, January 2021.
[5]A. G. Prabhu, A. Narayanan, and C. Kurian, "A Study on Security ISSUES in SaaS Cloud Computing," 2021.
[6] H. P. Singh, R. Singh, and V. Singh, "Cloud computing security issues, challenges and solutions," Easy Chair, pp. 2516-2314, 2020.
[7] A. Kumar and K. A. Kumar, "A Survey on Cloud Computing Security Threats, Attacks and Countermeasures: A Review," International Journal of Human Computations & Intelligence, vol. 1, no. 3, pp. 13-18, 2022.
[8] N. B. Muhammad and M. Bazzi, "Advances in Cloud Computing: Security Issues and Challenges in the Cloud," in 2022 5th International Conference on Information and Computer Technologies (ICICT), 2022: IEEE, pp. 110-116.
[9] A. H. Shaikh and B. Meshram, "Security issues in cloud computing," in Intelligent Computing and Networking: Proceedings of IC-ICN 2020, Springer, pp. 63-77, 2021.
[10] I. Indu, P. R. Anand, and V. Bhaskar, "Identity and access management in cloud environment: Mechanisms and challenges," Engineering science and technology, an international journal, vol. 21, no. 4, pp. 574-588, 2018.
[11] A. Sunyaev and A. Sunyaev, "Cloud computing," Internet Computing: Principles of Distributed Systems and Emerging Internet-Based Technologies, pp. 195-236, 2020.
[12] v. Shahi and M. Naqvi, "Investigation and evaluation of new models of data security in cloud computing," Non-functional Defense Quarterly, vol. 8, no. 2, pp. 35-42, 2017.
[13] K. Abbas, "DDoS Survey and Arrangements," 2019.
[14] P. Kumar, "Cloud computing: threats, attacks and solutions," International Journal of Emerging Technologies in Engineering Research (IJETER), vol. 4, no. 8, pp. 24-28, 2016.
[15] D. Stiawan, M. E. Suryani, M. Y. Idris, M. N. Aldalaien, N. Alsharif, and R. Budiarto, "Ping flood attack pattern recognition using a K-means algorithm in an Internet of Things (IoT) network," IEEE Access, vol. 9, pp. 116475-116484, 2021.

پایگاه‌های اینترنتی:

[16] A Comprehensive Guide to Cloud Security in 2023 (Risks, Best Practices, Certifications) Edward Jones, October 28, 2022.
[17] Cloud Computing Security Issues https://www.skyhighsecurity.com/en-us/cybersecurity-defined/cloud-computing-security-issues
[18] Gartner Security and Risk Management Summit https://www.gartner.com/en/conferences/emea/security-risk-management-uae/featured-topics/cloud-security
[19] What is a cloud firewall? What is firewall-as-a-service (FWaaS)? https://www.cloudflare.com/learning/cloud/what-is-a-cloud-firewall/