دانشگاه آزاد اسلامی واحد الکترونیکی
مجله مدیریت اطلاعات، امنیت و سیستم ها
ISSN: 3060-6055

چالش های امنیتی در حوزه رایانش ابری

کیارش محمودنهرانی[1]، محسن حیدری[2] و محمد بغدادی[3]

[1]دانشجوی کارشناسی ارشد،دانشکده فنی مهندسی،دانشگاه آزاد اسلامی- واحد تهران غرب،تهران،ایران

[2]دانشجوی کارشناسی ارشد،دانشکده فنی مهندسی،دانشگاه آزاد اسلامی- واحد تهران غرب،تهران،ایران

[3]دانشجوی کارشناسی ارشد،دانشکده فنی مهندسی،دانشگاه آزاد اسلامی- واحد تهران غرب،تهران،ایران

چکیده:

به‌موازات رشد و گسترش تکنولوژی اطلاعات، مقوله امنیت در شبکه‌های ابری، به‌طور چشمگیری مورد توجه قرار گرفته است. امروزه امنیت به‌عنوان یکی از مهمترین چالش‌های فناوری رایانش ابری، مورد مطالعه محققان است. مهمترین گام در تامین امنیت، تشخیص تهدیدات احتمالی و ارایه فرایند امنیتی و محافظتی لازم است.در این فناوری، ابر، ابزاری است برای برون سپاری خدمات و باعث فراهم آمدن امکان استفاده تخصصی تر و کاراتر از منابع می‌شود. این مقاله چالش‌های امنیتی در بستر رایانش ابری را مورد بررسی قرار داد و نشان داد که احراز هویت کاربران یک گام حیاتی برای افزایش امنیت در ابر است. تکنیک‌های موجود برای احراز هویت کاربران شامل روش‌های سنتی مانند رمزهای عبور و پین‌ها هستند که به دانش کاربر متکی‌اند. روش‌های امن‌تر مانند احراز هویت چندعاملی چندین شکل تاییدیه از جمله رمزهای عبور، کارت‌های هوشمند و بیومتریک را ترکیب می‌کنند. علاوه بر این، روش‌هایی مانند رمزهای یک‌بار مصرف و تحلیل ضربه‌های کلید با تولید کدهای زمان‌دار و تحلیل الگوهای تایپ، امنیت را افزایش می‌دهند. تکنیک‌هایی مانند ماژول قابل اعتماد موبایل با توابع هش و رمزنگاری نامتقارن، احراز هویت چندعاملی با الگوریتم‌های رمزنگاری فازی هش و تحلیل ضربه‌های کلید با الگوریتم‌های خوشه‌بندی k-means نیز به کار می‌روند. همچنین، احراز هویت یک‌باره با پروتکل OTP و احراز هویت بیومتریک با سیستم احراز هویت استاتیک ارائه شده‌اند.

کلمات کلیدی: رایانش ابری، چالش‌های امنیتی رایانش ابری، احراز هویت، کنترل دسترسی، Cloud API

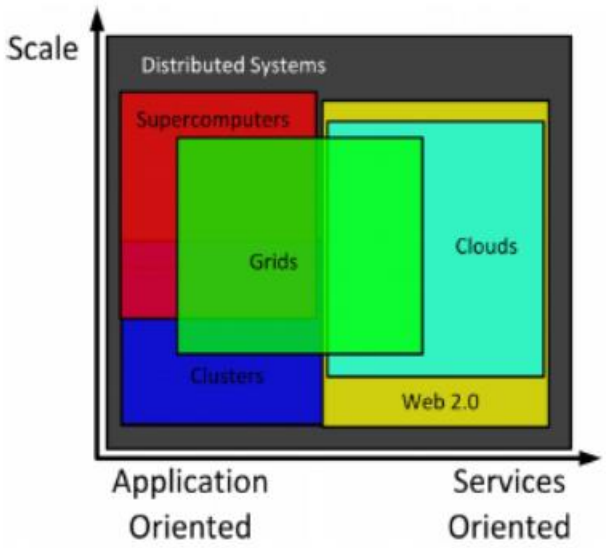
1. مقدمه

رایانش ابری یک مدل قوی است که به کاربران و سازمان‌ها اجازه می‌دهد خدمات مورد نیاز خود را براساس نیاز خود خریداری کنند. این مدل، خدمات بسیاری مانند ذخیره‌سازی، پلتفرم‌های استقرار، دسترسی راحت به سرویس‌های وب و غیره را ارایه می‌دهد. تعادل بار یک مشکل رایج در فضای ابری است که حفظ عملکرد برنامه‌های کاربردی مجاور اندازه‌گیری کیفیت خدمات(QoS[1]) و پیروی از سند توافقنامه سطح سرویس(SLA[2]) را که از سوی ارایه‌دهندگان ابری به شرکت‌ها نیاز است، دشوار می‌کند. هدف ارایه‌دهندگان ابر،

[1] Quality of Service
[2] Service Level Agreement

دانشگاه آزاد اسلامی واحد الکترونیکی
مجله مدیریت اطلاعات، امنیت و سیستم ها
ISSN: 3060-6055

توزیع بار کاری برابر بین سرورها است[1]. ویژگی‌های رایانش ابری با بسیاری از فناوری‌های موجود دیگر مانند رایانش شبکه‌ای، رایانش کاربردی، رایانش خوشه‌ای و رایانش توزیع‌شده به طور کلی همپوشانی دارد. در واقع، رایانش ابری از رایانش شبکه‌ای تکامل یافته و به عنوان عضو اصلی و پشتیبانی زیرساختی به آن متکی است. این تکامل، نتیجه تغییر در تمرکز از زیرساختی که منابع ذخیره‌سازی و محاسباتی ارائه می‌دهد (مانند مورد در شبکه‌ها) به زیرساختی است که بر اساس اقتصاد طراحی شده و هدف آن ارائه منابع و خدمات انتزاعی‌تر است (مانند مورد در ابرها). اما در مورد رایانش کاربردی، این یک الگوی جدید زیرساخت رایانشی نیست؛ بلکه یک مدل تجاری است که در آن منابع رایانشی، مانند محاسبات و ذخیره‌سازی، به‌صورت خدمات اندازه‌گیری‌شده و بسته‌بندی‌شده مشابه یک خدمت عمومی فیزیکی، مانند برق یا شبکه تلفن عمومی ارائه می‌شوند. رایانش کاربردی معمولاً با استفاده از سایر زیرساخت‌های رایانشی (مثلاً شبکه‌ها) با خدمات اضافی حسابداری و نظارت پیاده‌سازی می‌شود. یک زیرساخت ابری می‌تواند به صورت داخلی توسط یک شرکت استفاده شود یا به عنوان رایانش کاربردی به عموم عرضه شود. شکل 1، نمای کلی از رابطه بین ابرها و حوزه‌های دیگر را که با آن‌ها همپوشانی دارند، نشان می‌دهد. وب 2.0 تقریباً تمام طیف برنامه‌های خدمات‌محور را پوشش می‌دهد که در آن رایانش ابری در سمت مقیاس بزرگ قرار دارد. ابررایانه‌ها و رایانش خوشه‌ای بیشتر بر برنامه‌های غیرخدماتی سنتی متمرکز شده‌اند. رایانش شبکه نیز با همه این زمینه‌ها همپوشانی دارد که به طور کلی در مقیاس کمتری نسبت به ابررایانه‌ها و ابرها در نظر گرفته می‌شود [2].

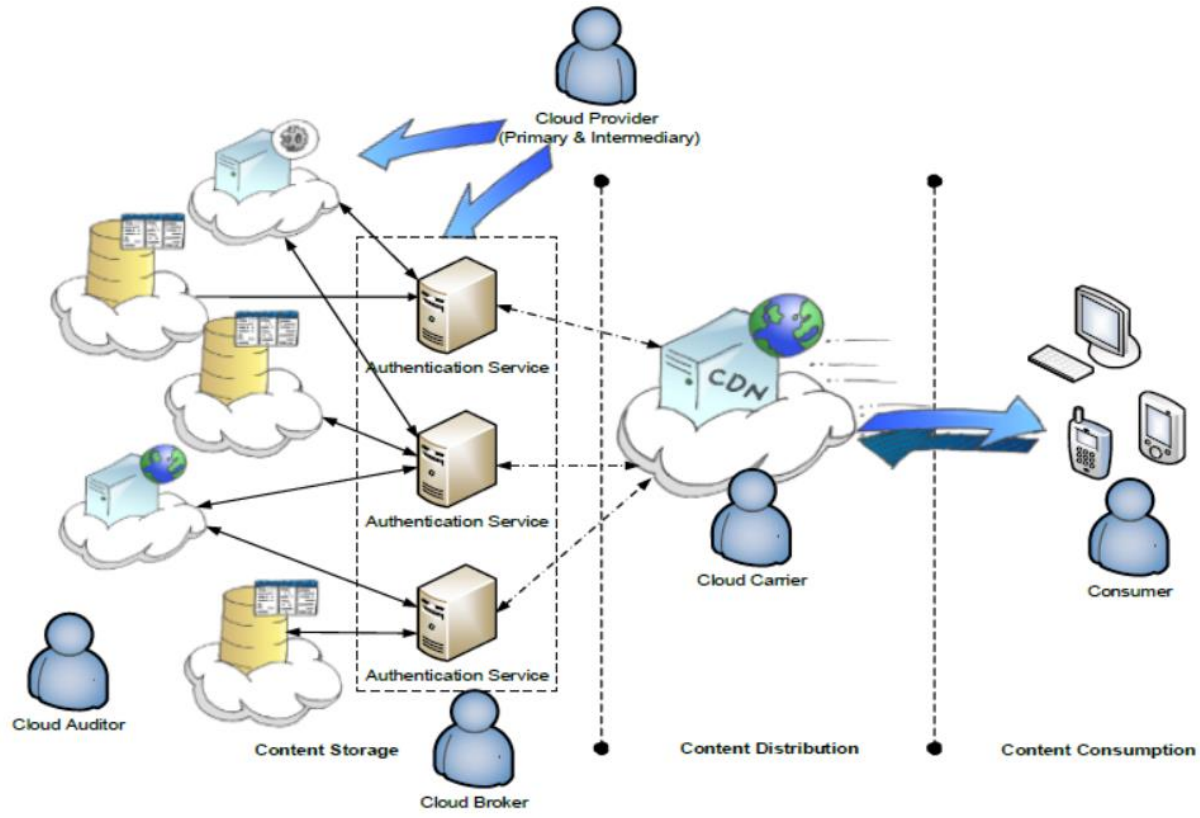


شکل 1. نمایی از شبکه‌ها و ابرها

ماهیت توزیع‌شده‌ی محیط ابری چالش‌هایی را در مدیریت هویت کاربران، احراز هویت و مجوزدهی ایجاد می‌کند. ارائه‌دهندگان خدمات ابری به اطلاعات ذخیره‌شده توسط کاربران برای احراز هویت دسترسی دارند که این موضوع مشکلات حریم خصوصی را به

دانشگاه آزاد اسلامی واحد الکترونیکی
مجله مدیریت اطلاعات، امنیت و سیستم ها
ISSN: 3060-6055

دنبال دارد. کاربران برای اطمینان از اجرای صحیح قوانین توافق‌نامه سطح خدمات (SLA[1]) با مشکل مواجه هستند، زیرا شفافیت کافی برای پایش(مانیتورینگ) اطلاعات خود در ابر وجود ندارد. علاوه بر این، کاربران که اطلاعات را در قالب چندین سرویس ابری مشترک به اشتراک گذاشته‌اند، باید رمزهای عبور را در هر سرویس برای احراز هویت ذخیره کنند. در نتیجه، داده‌های احراز هویت در چندین ابر تکرار می‌شوند که این مساله ممکن است امنیت را به خطر بیندازد. ارائه‌دهندگان خدمات ابری، مدیریت و احراز هویت کاربران را به طور فزاینده‌ای پیچیده می‌دانند که بر اعتماد کاربران تأثیر می‌گذارد. برای حل این مشکلات، راه‌حل‌هایی مانند امنیت به‌عنوان یک سرویس (SEaaS[2]) و احراز هویت به‌عنوان یک سرویس (AaaS[3]) پدید آمده‌اند که اقدامات امنیتی مبتنی بر ابر را ارائه می‌دهند. در شکل (2)، تمامی ذی‌نفعان در فرآیند احراز هویت سرویس ابری نشان داده شده است [3].



شکل 2. ذی‌نفعان در احراز هویت سرویس ابری

خدمات ابری به راحتی با داشتن یک مرورگر و اتصال به اینترنت قابل دسترسی هستند و از سرویس‌های محبوب مانند جیمیل، فیسبوک و دراپ‌باکس در دستگاه‌های مختلف پشتیبانی می‌کنند. یکی از مزایای مهم رایانش ابری این است که زیرساخت و نگهداری

[1] Service Level Agreement
[2] Security-as-a-Service
[3] Authentication-as-a-Service

دانشگاه آزاد اسلامی واحد الکترونیکی
مجله مدیریت اطلاعات، امنیت و سیستم ها
ISSN: 3060-6055

آن توسط ارائه‌دهندگان شخص ثالث مدیریت می‌شود. با این حال، رایانش ابری با تهدیدات امنیتی روبروست، از جمله حملات انکار سرویس توزیع‌شده (DDoS[1]) که می‌توانند خدمات را با ارسال درخواست‌های کاذب به سرورها مختل کنند و آن‌ها را برای کاربران قانونی غیرقابل دسترسی کنند. علی‌رغم مزایا، اطمینان از اجرای تدابیر امنیتی قوی برای حفاظت از داده‌ها و حفظ قابلیت اطمینان خدمات بسیار حیاتی است[4]. از مهمترین چالش‌های امنیتی در بستر ابر می توان به نفوذ داده‌ها، انطباق با مقررات قانونی و پاسخ‌گویی پیچیده به برخی رویدادها اشاره کرد. نفوذ داده‌ها می‌تواند به دلیل تدابیر امنیتی ناکافی یا آسیب‌پذیری‌های زیرساخت ابری رخ دهد که به از دست دادن اطلاعات حساس و ضرر مالی منجر می‌شود. انطباق با قوانین حفاظت از داده‌ها، پیچیده و پرهزینه است. علاوه بر این، کاربران مشترک چندین سرویس ابری با داده‌های احراز هویت تکراری در ابرهای مختلف مواجه می‌شوند که خطرات امنیتی را افزایش می‌دهد. پرداختن به این چالش‌ها برای حفاظت از داده‌ها و حفظ اعتماد در محیط‌های رایانش ابری بسیار حیاتی است[3] . از این رو، در این مقاله تلاش می شود به بررسی چالش‌های امنیتی در حوزه رایانش ابری پرداخته شود. درک این چالش‌ها به توسعه تدابیر امنیتی قوی برای حفاظت از اطلاعات حساس، حفظ اعتماد کاربران و اطمینان از انطباق قانونی کمک می‌کند.

2. الزامات دسترسی به محیط ابری

محیط ابری یک فضای چندکاربر و ناهمگون است که در آن ارائه‌دهندگان خدمات ابری (CSPها[2]) خدمات متنوعی را به صورت همزمان به بسیاری از مشتریان یا کاربران ارائه می‌دهند. این پارادایم مزایای قابل توجهی دارد، اما به این معنی است که الزامات کنترل دسترسی با آنچه معمولاً در شبکه‌های سازمانی عمومی استفاده می‌شود متفاوت است. عوامل کلیدی که باید در محیط ابری مورد توجه قرار گیرند شامل مکانیزم‌های کنترل دسترسی ویژه برای مدیریت نیازهای متنوع کاربران و اطمینان از ارائه خدمات امن و کارآمد می شوند. این الزامات در جدول 1 خلاصه شده اند [2]:

جدول1. الزامات دسترسی به محیط ابری

الزامات	توضیح
مستاجر[3]	مشتریان مختلف یک برنامه مدیریت ارتباط با مشتری ارائه‌شده توسط Salesforce.com ، مانند خدمات MRF ، BIT Mesra و بیمارستان‌های آپولو، به عنوان مستاجر محسوب می‌شوند. هر سازمان می‌تواند تعداد زیادی کاربر داشته باشد.
کاربر	کارمندان هر مستاجر که از برنامه‌های مختلف ابری استفاده می‌کنند.
وظیفه	ساده‌ترین یا اساسی‌ترین واحد، یک فرآیند کسب و کار به حساب می‌اید.

[1] Distributed Denial of service
[2] Cloud Service Providers
[3] Tenant

اشیاء	منابع مختلفی که کاربران مایل به دسترسی به آن‌ها هستند.
نقش	به هر کاربر در یک سازمان، بر اساس فعالیت‌هایی که مجاز به انجام آن‌ها است، اختصاص داده می‌شود
مجوز	منظور، مجوز انجام یک عملیات خاص بر روی یک شیء است
جلسه	منظور، نقشه کاربر به نقش‌های مختلف اختصاص داده شده به آن است.
مکان	مجوزهای دسترسی آگاه به مکان را در خود جای داده است.
قوانین کسب و کار	عملکردهای استاندارد یک سازمان که کاربران آن دنبال می‌کنند. این قوانین می‌توانند از یک سازمان به سازمان دیگر متفاوت باشند. این قوانین شامل کمترین دسترسی، کمترین جداسازی وظیفه، و تفویض وظایف است.

3. چالش‌های امنیتی رایانش ابری

در دنیای به هم پیوسته امروزی، فناوری ابری به عنوان عاملی حیاتی برای نوآوری صنعت فناوری اطلاعات در نظر گرفته می‌شود. این فناوری، مدلی است که خدمات مختلف بر اساس تقاضا و دسترسی شبکه به پایگاه‌های داده مشترک منابع فیزیکی مانند محاسبات و ذخیره‌سازی را در اختیار مصرف‌کنندگان قرار می‌دهد. به این ترتیب، مشتریان دیگر نیازی به خرید سخت افزار گران قیمت برای دسترسی به این خدمات ندارند. حال آن‌که، می‌توانند از سخت‌افزار کالایی (مانند لپ‌تاپ) متصل به اینترنت استفاده کنند و ابزاری با هدف توسعه راه‌حل‌هایی برای مشکلات پیچیده در اختیارشان بگذارند. علاوه بر این، رایانش ابری، کاربران را قادر می‌سازد تا از راه دور به منابع از هر مکانی دسترسی داشته باشند و امکان همکاری مجازی را فراهم می‌کند. این بستر مجموعه‌ای از خدمات مانند نرم افزار به عنوان سرویس(SaaS) ، پلتفرم به عنوان سرویس (PaaS) و زیرساخت به عنوان سرویس (IaaS) را ارائه می‌دهد. علاوه بر این، خدمات ابری مقیاس‌پذیر، انعطاف‌پذیر و قابل اعتماد برای کاربران در صورت تقاضا هستند [5]. از آنجا که میزان جرایم سایبری در اینترنت در حال افزایش است، امنیت رایانش ابری نیز به دلایل زیادی تحت تاثیر قرار گرفته است. به منظور محافظت از تمام خدمات و مزایای ارائه شده توسط رایانش ابری و اینترنت، امنیت داده ها ضروری است. محرمانه بودن داده‌ها را می‌توان در سراسر شبکه با استفاده از فناوری رمزنگاری-که رمزگذاری و رمزگشایی است- به دست آورد. از مهمترین دلایل ارزیابی امنیت در بستر ابری می‌توان به موارد جدول (2) اشاره کرد [6]:

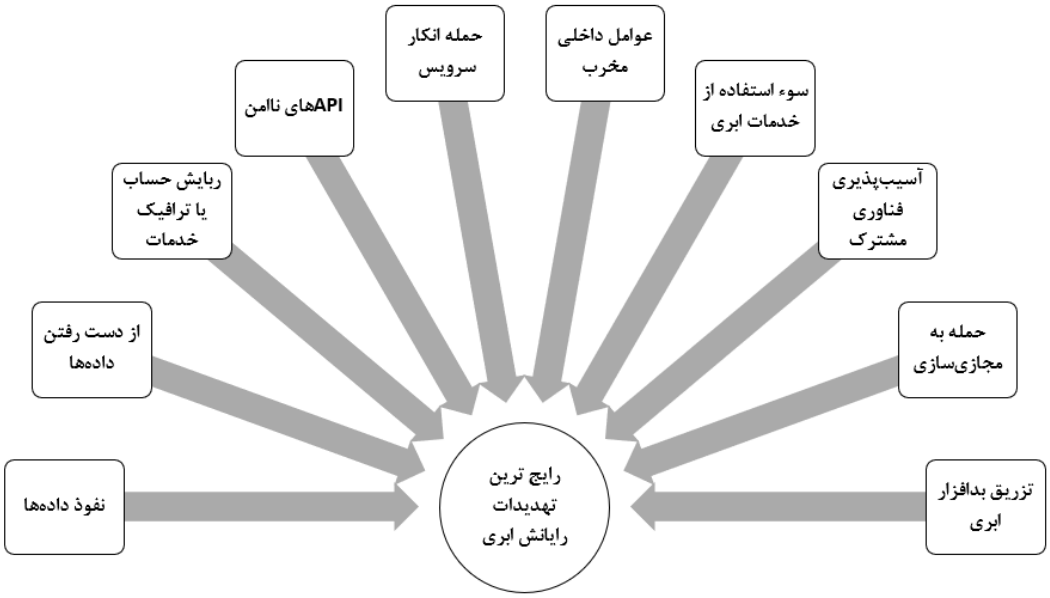
جدول2. اهمیت امنیت در بستر ابری

عامل	تعریف
احراز هویت	هویت فرستنده و گیرنده باید قبل از ارسال پیام تأیید شود.

دانشگاه آزاد اسلامی واحد الکترونیکی
مجله مدیریت اطلاعات، امنیت و سیستم ها
ISSN: 3060-6055

محرمانه بودن	فقط کاربران مجاز می‌توانند پیام را تفسیر کنند و هیچ کس دیگری نمی‌تواند از آن استفاده کند.
یکپارچگی	اطمینان از اینکه محتوای داده‌های ارسالی حاوی هیچ‌گونه تغییری نیست.
قابلیت اطمینان و در دسترس بودن سرویس	از آنجایی که مزاحمان بر دسترسی کاربران به خدمات تأثیر می‌گذارند، این فناوری باید کیفیت خدمات مورد انتظار را برای کاربران فراهم کند.
امنیت دسترسی به داده ها و محرمانگی	با ذخیره کردن پرونده‌های محرمانه امنیتی توسط سرویسی مثل Google docs بسیار می‌توان از امن ماندن و عدم دسترسی‌های غیر مجاز اطمینان حاصل کرد
مفقود شدن و از بین رفتن داده‌ها	با توجه به اینکه تعداد کمی از کاربران از داده‌های خود Back up می‌گیرند در صورتی که مشکلی برای cloud پیش بیاید کل داده‌ها از دست خواهد رفت.

اگرچه رایانش ابری یک پیشرفت در چندین سرویس وب موجود است، اما با تهدیدات امنیتی مشابه و متفاوت بسیاری روبه‌رو است که به سایر سرویس‌های وب مرتبط است. برخی از تهدیدات اصلی رایانش ابری در شکل 3 ارائه شده و در اینجا مورد بحث قرار گرفته‌اند[7] .



شکل 3. مهمترین تهدیدهای رایانش ابری

1.3 نفوذ داده‌ها

در رایانش ابری، داده‌ها از کاربران و سازمان‌های مختلف در محیط ابری ذخیره می‌شود و هرگونه نفوذ به این محیط یک حمله بالقوه به داده‌های همه کاربران ابر است. بنابراین، داده‌هایی که در محیط ابری ذخیره، پردازش یا به اشتراک گذاشته می‌شوند، هدف بسیار ارزنده‌ای هستند. این شامل نفوذهایی به دلیل غفلت یا خطای انسانی، حملات مخرب هدفمند، آسیب‌پذیری‌های مربوط به برنامه‌های ابری و سایر نواقص سیاست‌های امنیتی در تشخیص تهدیدات، کاهش آسیب‌پذیری‌ها، هوش امنیتی و بسیاری موارد دیگر است[7] .

2.3 از دست رفتن داده‌ها

یکی از خطرات بزرگ مرتبط با استفاده از ابر، از دست رفتن داده‌ها است. داده‌ها می‌توانند به روش‌های مختلفی به خطر بیفتند، از جمله حذف و تغییر محتوای اصلی. از دست رفتن داده‌ها به دلیل ویروس یا بدافزار که به سخت‌افزار، ذخیره‌سازی پشتیبان و بازیابی داده‌ها آسیب می‌رساند، در محیط ابری بسیار مشکل‌ساز است. این خطر همچنین می‌تواند به دلیل بلایای طبیعی، قطعی برق، خطای انسانی و خرابی هارد دیسک رخ دهد[7].

3.3 ربایش حساب یا ترافیک خدمات[1]

هک کردن اطلاعات حساس مربوط به حساب‌ها و خدمات توسط مجرمان سایبری یا هکرها دارای همان خطراتی است که بسیاری از خدمات دیگر وب با آن مواجه هستند. اطلاعات خصوصی مانند سوابق مالی، تصاویر، شماره کارت‌های اعتباری و غیره می‌توانند توسط هکرها منتشر، استفاده یا به فروش برسند. همچنین این تهدید شامل حملات مرد میانی[2]، دستکاری‌های مهندسی اجتماعی[3]، استراق سمع فعالیت‌ها[4] و نفوذ بدافزارها/جاسوس‌افزارها است[7].

4.3 رابط‌ها و واسط‌های برنامه‌نویسی کاربردی (API[5]) ناامن

رابط‌ها وAPI های ناامن و ماشین‌های مجازی (VM[6]) نیز یک تهدید بالقوه برای محیط رایانش ابری محسوب می‌شوند. API ها، VMها و سایر واسط‌های نرم‌افزاری توسط کاربر برای دسترسی به خدمات ابری استفاده می‌شوند. این نقاط تماس اجزای مرکزی هستند زیرا نظارت بر فعالیت‌ها، مدیریت و تأمین منابع را فراهم می‌کنند. بنابراین، نقایص امنیتی در این نقاط منجر به کنترل‌های دسترسی نادرست، احراز هویت غیرقانونی، نقض رمزنگاری و غیره می‌شود. این خطرات به دلیل ضعف در اعتبارنامه‌هایAPI ، نارسایی در مدیریت کلیدها، اشکالات در سیستم عامل، نرم‌افزارهای بدون پچ و خطاهای هایپروایزر[7] به‌وجود می‌آیند[7].

[1] Account or service traffic hijacking
[2] Man-in-the-middle attack
[3] Social engineering manipulations
[4] Eavesdropping on activities
[5] Application programme interfaces
[6] Virtual machines
[7] Hypervisor

5.3 حمله انکار سرویس (DoS)

در یک حمله DoS، شبکه توسط اسپم‌های مهاجم غرق می‌شود که ترافیک بی‌فایده‌ای با هدف استفاده از منابع ایجاد می‌کند. این وضعیت می‌تواند منجر به عدم دسترسی منابع و خدمات برای کاربران معتبر شود. این حمله به دلیل معماری ضعیف امنیت شبکه، برنامه‌های آسیب‌پذیر، پروتکل‌های شبکه ناامن و غیره رخ می‌دهد[7].

6.3 عوامل داخلی مخرب

همچنین تهدیدات امنیتی می‌توانند داخلی باشند و این نوع تهدیدها کمی سخت‌تر قابل پیشگیری هستند. هر اطلاعات حساسی می‌تواند توسط هر داخلی/کارمندی که دسترسی مدیریتی دارد به یک دستگاه ذخیره‌سازی کپی شود. اطلاعات می‌توانند توسط هر کارمند سابق ناراضی، مدیر سیستم، شریک تجاری یا پیمانکار شخص ثالث به سرقت بروند. چنین ریسک‌هایی می‌توانند با انجام بررسی‌های پیش‌زمینه‌ای مناسب و محدود کردن دسترسی به داده‌های محرمانه کاهش یابند [7].

7.3 سوء استفاده از خدمات ابری

ابر به کاربران خود توهم قابلیت نامحدود محاسباتی، منابع شبکه و ظرفیت ذخیره‌سازی را ارائه می‌دهد. اسپمرها، نویسندگان کد مخرب، هکرها و سایر مجرمان سایبری می‌توانند از این قابلیت‌ها به طور ناعادلانه برای شکستن رمز عبور یا کلید رمزنگاری، ایجاد گلوگاه در شبکه، میزبانی داده‌های مخرب و بسیاری موارد دیگر استفاده کنند. این تهدید می‌تواند به دلیل نبود نظارت مناسب و توافق‌نامه سطح خدمات در محیط ابری بروز کند [7].

8.3 آسیب‌پذیری‌های فناوری مشترک

رایانش ابری یک فناوری مقیاس‌پذیر برای به اشتراک‌گذاری زیرساخت، فناوری و منابع است. این پلتفرم چندکاربری از هایپروایزر برای تسهیل دسترسی به سیستم‌عامل‌های میهمان استفاده می‌کند. با این حال، کمبودهای مجوزدهی و محدودیت‌های هایپروایزر می‌توانند به نفوذگران دسترسی و کنترل نامناسب را فراهم کنند. همچنین این تهدید می‌تواند به دلیل آسیب‌پذیری‌های مرتبط با ماشین‌های مجازی و سوییچینگ شخص ثالث بروز کند [7].

9.3 حمله مجازی‌سازی[1]

معماری مجازی‌سازی داخلی نیاز به سخت‌افزار مستقل دارد و بهترین مجازی‌سازی با استفاده از معماری لایه‌ای برنامه‌ریزی شده است. با وجود ناهنجاری‌ها و دشمنان در سیستم‌عامل‌های امروزی، می‌توان آسیب‌پذیری‌هایی را برای کنترل مخرب سیستم‌عامل میزبان راه‌اندازی کرد. به محض اینکه مهاجم توانایی کنترل سیستم‌عامل میزبان را به دست آورد، هایپروایزر به عنوان ناهنجاری

[1] Virtualisation attack

مشخص می‌شود. بنابراین، حقوق مدیریتی فرمان هایپروایزر به مهاجم اجازه می‌دهد تا هر اقدام مخربی را بر روی هر یک از ماشین‌های مجازی که توسط هایپروایزر میزبانی می‌شوند انجام دهد [7].

10.3 تزریق بدافزار ابری

حملات تزریق بدافزار ابری (CMIA[1]) برای دسترسی به داده‌های کاربر که در ابر ذخیره و پردازش می‌شوند صورت می گیرند. برخی از تهدیدات CMIA که به طور گسترده اعمال می‌شوند شامل حملات اسکریپت‌نویسی سایت و حملات تزریق زبان پرس و جو ساخت‌یافته (SQL[2]) هستند. چنین حملاتی ممکن است به دلیل ارائه‌دهندگان خدمات ابری آسیب‌پذیر مانند پلتفرم ابری OpenStack رخ دهند. با کمک یک کد مخرب، دشمنان می‌توانند به راحتی اطلاعات رمزگذاری شده را از بافر از طریق سوء استفاده از نقص طراحی در رایانه‌های اصلی امروزی ارسال کنند[7].

4. امنیت به عنوان یک سرویس (SaaS[3])

یکی از انواع خدمات ابری امنیت به عنوان سرویس (SaaS) است که راه‌حل‌های امنیتی ابری مانند تشخیص نفوذ، آنتی‌ویروس و مدیریت فایروال را از طریق اینترنت به کاربران ارائه می‌دهد. این رویکرد به سازمان‌ها اجازه می‌دهد نیازهای امنیتی خود را به ارائه‌دهندگان ابری متخصص واگذار کنند و از مقیاس‌پذیری، انعطاف‌پذیری و هزینه‌های کمتر رایانش ابری بهره‌مند شوند. SaaS می‌تواند با سیستم‌های داخلی موجود ادغام شود و نظارت مداوم و تشخیص تهدیدات در زمان واقعی را فراهم کند. این ادغام زیرساخت امنیتی کلی را تقویت می‌کند و به سازمان‌ها کمک می‌کند تا به‌طور کارآمدتری به الزامات انطباق دست یابند و با چشم‌انداز تهدیدات سایبری متغیر سازگار شوند[8]. یکی از انواع این نوع خدمات، احراز هویت به عنوان سرویس (AaaS) است. AaaS فرمی از احراز هویت کاربر است که از طریق آن خطر از دست دادن داده‌های محرمانه از ابر کاهش می‌یابد. هنگامی که یک کاربر خدمات ابری می‌خواهد به چندین سرویس موجود در ابر دسترسی پیدا کند، باید رمز عبور خود را در چندین ابر ذخیره کند که این موضوع مشکلات حریم خصوصی را برای مشتری و ارائه‌دهنده به همراه دارد [9].

تکنیک‌های احراز هویت مختلفی وجود دارد که برای ایمن‌سازی داده‌ها و احراز هویت کاربران قانونی اعمال می‌شوند. از مهمترین الزامات این نوع سرویس‌ها می توان به موارد زیر اشاره نمود:

- تکنیک امنیتی از نوعی باید اعمال شود که داده‌ها بدون گرفتن اجازه از شخص معتبر قابل تغییر نباشند.
- سیستمی امنیتی باید انتخاب شود که کاربران بتوانند به ایمنی و حفظ حریم خصوصی آن داده‌ها اعتماد کنند.
- داده‌ها باید همیشه در زمانی که به آن ها نیاز است در دسترس باشند.

[1] Cloud malware injection attacks
[2] Structured query language
[3] Security-as-a-Service

دانشگاه آزاد اسلامی واحد الکترونیکی
مجله مدیریت اطلاعات، امنیت و سیستم ها
ISSN: 3060-6055

- معمولاً احراز هویت یا تنها برای یک طرف است یا دسترسی باز است، ارائه‌دهنده خدمات ابری بستر مناسبی برای احراز هویت چندگانه رابط کاربری ندارد و این منجر به دسترسی غیرمجاز یا ضعیف به فضای ابری می‌شود [9].

1.4 تکنیک‌های موجود برای احراز هویت کاربر

تکنیک‌های موجود برای احراز هویت کاربران شامل روش‌های سنتی مانند رمزهای عبور و پین‌ها است که به چیزی که کاربر می‌داند متکی هستند. تکنیک‌های امن‌تر مانند احراز هویت چندعاملی (MFA[1]) چندین شکل تاییدیه را ترکیب می‌کند، از جمله رمزهای عبور، کارت‌های هوشمند و بیومتریک. علاوه بر این، روش‌هایی مانند رمزهای یک‌بار مصرف (OTP[2]) و تحلیل ضربه‌های کلید امنیت را با تولید کدهای زمان‌دار و تحلیل الگوهای تایپ افزایش می‌دهند. در جدول 3، تکنیک‌های موجود برای احراز هویت کاربر ارائه شده است [9].

جدول 3. تکنیک‌های موجود برای احراز هویت کاربر

تکنیک	الگوریتم/روش/ابزار	نتایج
ماژول قابل اعتماد موبایل	توابع هش، طرح‌های امضا، رمزنگاری نامتقارن	جنبه امنیتی مورد استفاده در تلفن‌های همراه
احراز هویت چندعاملی (MFA)	الگوریتم‌های رمزنگاری فازی هش	اعتبارسنجی کاربران معتبر و شناسایی متقلبان در مجموعه داده‌ها
تحلیل ضربه‌های کلید	الگوریتم‌های خوشه‌بندیk-means	نشان‌دادن قابلیت احراز هویت کاربران نهایی
احراز هویت یک‌باره	پروتکلOTP	پروتکل در برابر حملات رمز یک‌بار مصرف امن است
احراز هویت بیومتریک	سیستم احراز هویت استاتیک	احراز هویت هویت کاربران از طریق دستگاه‌های اسکن ویژه
رمزهای عبور برای احراز هویت کاربران عمومی	پنجرهVisual Crypto-Pass ، عبور گرافیکی	قابلیت استفاده و امنیت

همچنین در ادامه توضیح مختصری در مورد هر یک از تکنیک‌ها آورده شده است.

1.1.4 ماژول قابل اعتماد تلفن همراه[3]

[1] Multi-factor Authentication
[2] One-Time Password
[3] Mobile trusted module

دانشگاه آزاد اسلامی واحد الکترونیکی
مجله مدیریت اطلاعات، امنیت و سیستم ها
ISSN: 3060-6055

ماژول قابل اعتماد موبایل (MTM[1]) یک تکنیک پیشرفته احراز هویت کاربر است که برای بهبود امنیت دستگاه‌های موبایل طراحی شده است. این تکنیک از روش‌های رمزنگاری مانند توابع هش، طرح‌های امضا و رمزنگاری نامتقارن برای حفاظت از داده‌ها و تایید هویت کاربران استفاده می‌کند. MTM یک محیط امن برای عملیات حساس از جمله تولید کلید و ذخیره اعتبارنامه‌ها فراهم می‌کند و با جداسازی عملکردهای امنیتی حیاتی از آسیب‌پذیری‌های نرم‌افزاری ممکن، خطر دسترسی غیرمجاز و نقض داده‌ها را کاهش می‌دهد. این تکنیک از احراز هویت چندعاملی پشتیبانی می‌کند و عوامل اضافی مانند بیومتریک را برای افزایش امنیت اضافه می‌کند. MTM به صورت یکپارچه با سیستم‌عامل‌های تلفن همراه ادغام می‌شود و فرایندهای احراز هویت کارامد و کاربرپسند را تضمین می‌کند و همزمان خطر دسترسی غیرمجاز و نقض داده‌ها را کاهش می‌دهد [10].

2.1.4 احراز هویت چندعاملی (MFA[2])

احراز هویت چندعاملی (MFA) یک تکنیک امنیتی است که نیاز به چندین شکل شناسایی دارد و شامل موردی که کاربر می‌داند (مانند رمز عبور)، موردی که کاربر دارد (مانند گوشی هوشمند)، و موردی که کاربر است (مانند بیومتریک) می‌شود. این رویکرد لایه‌ای خطر دسترسی غیرمجاز را به طور قابل توجهی کاهش می‌دهد و دسترسی به سیستم‌ها را برای مهاجمان بسیار سخت‌تر می‌کند. با ارائه یک لایه امنیتی اضافی، MFA کمک می‌کند تا اطلاعات حساس و سیستم‌های بحرانی محافظت شوند و خطرات مرتبط با احراز هویت تنها با رمز عبور مانند فیشینگ و سرقت رمز عبور کاهش یابد. این تکنیک به طور گسترده در صنایع مختلف برای افزایش امنیت و اعتماد در تراکنش‌های دیجیتال پذیرفته شده است [11].

3.1.4 تحلیل ضربه‌های کلید[3]

تحلیل ضربه‌های کلید یک تکنیک احراز هویت کاربر است که از الگوهای تایپ منحصر به فرد افراد برای تایید هویت آن‌ها استفاده می‌کند. با اندازه‌گیری ریتم، سرعت و فشار اعمال‌شده هنگام تایپ، یک "امضای ضربه‌کلید" متمایز برای هر کاربر ایجاد می‌شود. این روش بیومتریک، با استفاده از الگوریتم‌هایی مانند خوشه‌بندی K-means، امنیت را افزایش می‌دهد و تقلید یا جعل الگوهای تایپ را برای مهاجمان دشوار می‌کند. تحلیل ضربه‌های کلید احراز هویت مداوم را ارائه می‌دهد و حتی پس از ورود اولیه نیز تاییدیه مداوم را فراهم می‌کند و در محیط‌های با امنیت بالا بسیار مفید است. این روش، یک فرایند احراز هویت بی‌درز و نامحسوس را ارائه می‌دهد که تجربه کاربری را بهبود می‌بخشد و نیاز به سخت‌افزار اضافی ندارد[12].

4.1.4 احراز هویت یک‌باره (OTA[4])

احراز هویت یک‌باره (OTA) یک مکانیزم امنیتی است که برای هر جلسه ورود یک کد منحصر به فرد و زمان‌دار تولید می‌کند و امنیت را با اطمینان از اینکه هر جلسه نیاز به یک کد متفاوت دارد افزایش می‌دهد. این روش که به‌طور معمول از طریق پروتکل‌های

[1] Mobile Trusted Module
[2] Multi-factor Authentication
[3] Key stroke Analysis
[4] One time Authentication

رمز یک‌بار مصرف (OTP[1]) پیاده‌سازی می‌شود، یک کد منحصر به فرد را برای هر تلاش ورود به دستگاه ثبت‌شده کاربر ارسال می‌کند که فقط برای یک مدت کوتاه معتبر است. OTA با دشوار کردن استفاده مجدد از اعتبارنامه‌های دزدیده شده برای مهاجمان، خطر دسترسی غیرمجاز را به طور قابل توجهی کاهش می‌دهد. این روش به ویژه در محافظت از حساب‌های حساس و تراکنش‌های مالی مؤثر است و امنیت قوی و راحتی کاربر را حفظ می‌کند[13].

5.1.4 احراز هویت بیومتریک

احراز هویت بیومتریک از ویژگی‌های فیزیکی یا رفتاری منحصر به فرد مانند اثر انگشت، تشخیص چهره، اسکن عنبیه یا تشخیص صدا برای تأیید هویت کاربر استفاده می‌کند. این روش بسیار ایمن بوده، تقلید یا جعل آن سخت است و محافظت قوی در برابر دسترسی غیرمجاز فراهم می‌کند. سیستم‌های بیومتریک تجربه کاربری را با حذف نیاز به رمزهای عبور پیچیده و دستگاه‌های احراز هویت اضافی ساده می‌کنند. احراز هویت بیومتریک به طور گسترده در بخش‌های مختلف پذیرفته شده و اطمینان می‌دهد که تنها افراد مجاز می‌توانند به اطلاعات حساس دسترسی پیدا کنند و امنیت و راحتی را افزایش می‌دهد[14].

6.1.4 رمزهای عبور برای احراز هویت کاربران عمومی

رمزهای عبور برای احراز هویت کاربران عمومی یک روش گسترده است که شامل ایجاد یک رشته مخفی از کاراکترها برای دسترسی کاربران به سیستم‌ها و خدمات می‌شود. رمزهای عبور به دلیل سادگی و سهولت استفاده، محبوب هستند اما اثربخشی آن‌ها به پیچیدگی رمز عبور و پیروی از روش‌های امنیتی خوب بستگی دارد. با این حال، رمزهای عبور دارای آسیب‌پذیری‌های ذاتی هستندکه از جمله آنها، حساسیت به حملات فیشینگ، حملات جست‌وجوی فراگیر و سرقت است. برای افزایش امنیت، اقدامات اضافی مانند احراز هویت چندعاملی (MFA) توصیه می‌شود که رمزهای عبور را با اشکال دیگر تأییدیه ترکیب می‌کند. این رویکرد به محافظت از اطلاعات حساس کمک می‌کند و اطمینان می‌دهد که رمزهای عبور همچنان گزینه‌ای مناسب هستند در حالی که به محدودیت‌های آن‌ها رسیدگی می‌شود[15].

5. کارهای پیشین

گانجام و همکاران [2] به بررسی امنیت APIهای ابری که یکی از تهدیدات عمده در رایانش ابری است، پرداختند. مدل پیشنهادی علاوه بر استفاده از احراز هویت مبتنی بر شناسه و رمز عبور برای کاربران قانونی، سیاست‌های کنترل دسترسی را نیز به کار می‌گیرد تا از دسترسی غیرمجاز به قابلیت‌های APIهای ابری جلوگیری کند. لیم و همکاران [3] به‌طور انتقادی، راهبردها و چارچوب‌های مختلف احراز هویت برای خدمات ابری را مورد بررسی قرار دادند، مزایا و معایب آن‌ها را بحث کردند و طبقه‌بندی احراز هویت خدمات ابری پیشرفته را ارائه دادند. این مقاله با بررسی مسائل باز، چالش‌های اصلی و جهت‌های آینده در این زمینه را بررسی نموده است. شاهیل و همکاران [4] ریسک‌های حملات انکار سرویس توزیع شده (DDOS) را که می‌توانند با ارسال هزاران درخواست مخرب به

[1] One-Time Password

شبکه سرور یا بهره‌برداری از آسیب‌پذیری‌های نرم‌افزاری، سایت تولیدی را غیرقابل استفاده کنند، مورد بررسی قرار داده اند. این مقاله دو راهبرد پیشگیرانه یعنی فیلتر کردن ورودی و خروجی شبکه (NEIF)- که به جلوگیری از حملات DDOS از ابر کمک می‌کند- و تکنیک هانی‌پات را- که با ضبط فعالیت‌های مهاجم، حملات و مهاجمان را شناسایی می‌کند-، پیشنهاد نموده است. در این مقاله تأکید شده است که اگرچه این راهبردها مؤثر هستند، اما به دلیل خطرات ذاتی، نیاز به بهبود بیشتر دارند. الجمعه و همکاران [7] تهدیدات مختلف رایانش ابری را بررسی و مکانیزم‌های دفاعی در برابر این تهدیدات را مشخص کرده‌اند. بر اساس این مقاله، تهدید بزرگی که شناسایی شده، مربوط به نقض داده‌ها است که به دلیل عدم درک مدیریت از خدمات رایانش ابری و مکانیزم‌های دفاعی آن‌ها رخ می‌دهد. همچنین، این مطالعه سوء استفاده از خدمات رایانش ابری را نیز مطرح می‌کند که می‌تواند علاوه بر داده‌های حساس سازمان، هویت و اطلاعات شخصی کاربران را نیز به خطر بیندازد. شارما و همکاران [9] نتیجه گرفتند که برای پیاده‌سازی احراز هویت چندمرحله‌ای در محیط‌های ابری می توان از تکنیک‌هایی مانند دسترسی بیومتریک و سیستم‌های احراز هویت یک‌بار مصرف یا موبایلی استفاده نمود. این مطالعه بیان کرد که جامعه پژوهش علمی به طور گسترده‌ای تکنیک‌های احراز هویت موجود در محیط رایانش ابری را مورد بررسی قرار نداده است. این مطالعه فناوری‌ها و تکنیک‌های مختلف را نشان داده و مقایسه می‌کند و نیاز به تحقیقات بیشتر در مورد روش‌های احراز هویت کاربران و راهبردهای پیشگیری در محیط رایانش ابری را مورد تاکید قرار می‌دهد. آدی و همکاران [16] یک مدل امنیت داده پویا چهار مرحله‌ای برای رایانش ابری ارائه دادند که از رمزنگاری و استگانوگرافی استفاده می‌کند. این مدل شامل رمزگذاری، استگانوگرافی، پشتیبان‌گیری و بازیابی داده‌ها و نیز به اشتراک‌گذاری داده‌ها است. ثابیت و همکاران [17] یک الگوریتم رمزگذاری سبک وزن را برای بهبود امنیت داده‌ها در رایانش ابری پیشنهاد دادند که با استفاده از روش‌های معماری Feistal و عملیات منطقی امنیت قوی‌تری را فراهم می‌کند. لی و همکاران [18] یک سیستم تولید هوشمند با استفاده از رایانش لبه‌ای و بلاکچین طراحی کردند که می‌تواند زمان پردازش را بهبود بخشد و انتقال داده‌ها و معاملات خدمات تولیدی را تسهیل کند.

در جدول 4 خلاصه این مطالعات آورده شده است:

جدول 4. خلاصه پژوهش های پیشین

مرجع	هدف	راهکار پیشنهادی در زمینه امنیت ابری	نتیجه
گانجام و همکاران[2]	بررسی امنیتAPI های ابری	احراز هویت مبتنی بر شناسه و رمز عبور و استفاده از سیاست‌های کنترل دسترسی	سیاست‌های کنترل دسترسی از دسترسی غیرمجاز به APIهای ابری جلوگیری می‌کند

لیم و همکاران[3]	بررسی راهبردها و چارچوب‌های احراز هویت برای خدمات ابری	طبقه‌بندی سیستم های احراز هویت بر اساس هدف و کاربرد	نیاز به بررسی مسائل باز، چالش‌ها و جهت‌های آینده در احراز هویت خدمات ابری
شاهیل و همکاران[4]	بررسی ریسک‌های حملات DDOS	فیلتر کردن ورودی و خروجی شبکه (NEIF) و تکنیک هانی‌پات	این راهبردها مؤثر هستند اما نیاز به بهبود بیشتر دارند.
الجمعه و همکاران[7]	بررسی تهدیدات رایانش ابری و مکانیزم‌های دفاعی	شناسایی نقض داده‌ها به دلیل عدم درک مدیریت و سوء استفاده از خدمات ابری	تهدیدات می‌توانند داده‌های حساس سازمان و هویت کاربران را به خطر بیندازند.
شارما و همکاران[9]	پیاده‌سازی احراز هویت چندمرحله‌ای در محیط‌های ابری	استفاده از دسترسی بیومتریک و سیستم‌های احراز هویت یک‌بار مصرف یا موبایلی	نیاز به تحقیقات بیشتر در مورد روش‌های احراز هویت کاربران و راهبردهای پیشگیری در محیط رایانش ابری تأکید می‌شود.
آدی و همکاران[16]	ارائه مدل امنیت داده پویا چهار مرحله‌ای	رمزنگاری و استگانوگرافی شامل رمزگذاری، پشتیبان‌گیری، بازیابی داده‌ها و به اشتراک‌گذاری داده‌ها	مدل ارائه‌شده امنیت، حریم خصوصی و یکپارچگی داده‌ها را در برابر مهاجمان تضمین می‌کند.
ثابیت و همکاران[17]	بهبود امنیت داده‌ها در رایانش ابری	الگوریتم رمزگذاری سبک وزن با استفاده از روش‌های معماری Feistal و عملیات منطقی	الگوریتم پیشنهادی امنیت قوی‌تری را فراهم می‌کند
لی و همکاران[18]	طراحی سیستم تولید هوشمند با رایانش لبه‌ای و بلاکچین	استفاده از رایانش لبه‌ای برای کاهش زمان پردازش و بلاکچین برای تسهیل انتقال داده‌ها و معاملات خدمات تولیدی	سیستم پیشنهاد شده زمان پردازش را بهبود می‌بخشد و انتقال داده‌ها و معاملات خدمات تولیدی را تسهیل می‌کند.

دانشگاه آزاد اسلامی واحد الکترونیکی
مجله مدیریت اطلاعات، امنیت و سیستم ها
ISSN: 3060-6055

6. نتیجه گیری

با پیشرفت فناوری اطلاعات، نیاز به انجام کارهای محاسباتی در هر زمان و مکان افزایش یافته و همچنین نیاز به انجام محاسبات سنگین بدون نیاز به سخت‌افزارها و نرم‌افزارهای گران‌قیمت به وجود آمده است. رایانش ابری به عنوان آخرین پاسخ فناوری به این نیازها، به میلیون‌ها کاربر امکان می‌دهد داده‌های خود را در فضای عظیم ابری ذخیره کنند. با این حال، این راحتی همراه با خطراتی نظیر دسترسی غیرمجاز و از دست دادن داده‌ها است که امنیت را به چالشی بسیار مهم تبدیل می‌کند. رایانش ابری می‌تواند با استفاده از ماشین‌های مجازی شبکه‌ای به طور پویا مراکز داده جدید ایجاد کند و توسعه نرم‌افزارها به عنوان یک سرویس قابل دسترس برای میلیون‌ها نفر را تسهیل کند. تهدیدات امنیتی در رایانش ابری به دو دسته داخلی و خارجی تقسیم می‌شوند: تهدیدات خارجی شامل آسیب‌پذیری‌های مراکز داده بزرگ و تهدیدات داخلی شامل نیاز به حفاظت کاربران از یکدیگر است. رایانش ابری به کسب‌وکارها امکان کاهش هزینه‌ها از طریق برون‌سپاری خدمات مورد نیازشان را می‌دهد، اما چالش‌های جدیدی در حفاظت از داده‌ها، قابلیت اطمینان، یکپارچگی و محرمانه بودن را معرفی می‌کند. در نتیجه، امنیت ابری به یک تمایز کلیدی و مزیت رقابتی بین ارائه‌دهندگان ابر تبدیل شده است. با توجه به افزایش جرایم سایبری، امنیت رایانش ابری به دلایل مختلف به‌طور قابل‌توجهی تحت تأثیر قرار گرفته است. امنیت داده‌ها برای محافظت از تمامی خدمات و مزایای ارائه‌شده توسط رایانش ابری و اینترنت بسیار حائز اهمیت است. محرمانه بودن داده‌ها را می‌توان با استفاده از فناوری‌های رمزنگاری برای رمزگذاری و رمزگشایی در سراسر شبکه حفظ کرد. دلایل اصلی برای ارزیابی امنیت در بستر ابری شامل احراز هویت، اطمینان از اینکه فقط کاربران مجاز قادر به تفسیر پیام‌ها هستند؛ محرمانه بودن، حفظ یکپارچگی داده‌ها در برابر تغییرات غیرمجاز؛ قابلیت اطمینان و در دسترس بودن سرویس، تضمین کیفیت خدمات مورد انتظار با وجود تداخل‌ها؛ امنیت دسترسی به داده‌ها و محرمانگی، اطمینان از امن ماندن و عدم دسترسی غیرمجاز به فایل‌های محرمانه ذخیره‌شده در خدماتی مانند Google Docs؛ و پیشگیری از نابودی یا از دست دادن داده‌ها، با توجه به اینکه تعداد کمی از کاربران، از داده‌های خود نسخه پشتیبان تهیه می‌کنند و در صورت بروز مشکل برای ابر، کل داده‌ها از دست خواهند رفت. در این مقاله به بررسی چالش های امنیتی در بستر ابری پرداخته شد. نتایج نشان داد؛ احراز هویت کاربران یک گام کلیدی در افزایش امنیت ابر است. همچنین تکنیک‌های موجود برای احراز هویت کاربران شامل روش‌های سنتی مانند رمزهای عبور و پین‌ها است که به چیزی که کاربر می‌داند متکی هستند. تکنیک‌های امن‌تر مانند احراز هویت چندعاملی چندین شکل تاییدیه، از جمله رمزهای عبور، کارت‌های هوشمند و بیومتریک را ترکیب می‌کند. علاوه بر این، روش‌هایی مانند رمزهای یک‌بار مصرف و تحلیل ضربه‌های کلید امنیت را با تولید کدهای زمان‌دار و تحلیل الگوهای تایپ افزایش می‌دهند. در این میان، تکنیک‌هایی مانند ماژول قابل اعتماد تلفن همراه با توابع هش و رمزنگاری نامتقارن، احراز هویت چندعاملی با الگوریتم‌های رمزنگاری فازی هش و تحلیل ضربه‌های کلید با الگوریتم‌های خوشه‌بندی k-means نیز استفاده می‌شوند. همچنین، احراز هویت یک‌باره با پروتکل OTP و احراز هویت بیومتریک با سیستم احراز هویت استاتیک ارائه شده‌اند.

منابع

[1] Shafiq DA, Jhanjhi NZ, Abdullah A. Load balancing techniques in cloud computing environment: A review. Journal of King Saud University-Computer and Information Sciences. 2022 Jul 1;34(7):3910-33.

[2] Gunjan K, Tiwari RK, Sahoo G. Towards securing APIs in cloud computing. arXiv preprint arXiv:1307.6649. 2013 Jul 25.

[3] Lim SY, Kiah MM, Ang TF. Security issues and future challenges of cloud service authentication. Acta Polytechnica Hungarica. 2017 May;14(2):69-89.

[4] Shahil UM, Deekshitha M, Anam M N, Basthikodi M. Ddos attacks in cloud computing and its preventions. JETIR-International Journal of Emerging Technologies and Innovative Research (www. jetir. org), ISSN. 2019 May 5:2349-5162.

[5] Rahman A, Islam MJ, Band SS, Muhammad G, Hasan K, Tiwari P. Towards a blockchain-SDN-based secure architecture for cloud computing in smart industrial IoT. Digital Communications and Networks. 2023 Apr 1;9(2):411-21.

[6] Thabit F, Can O, Alhomdy S, Al-Gaphari GH, Jagtap S. A Novel Effective Lightweight Homomorphic Cryptographic Algorithm for data security in cloud computing. International Journal of intelligent networks. 2022 Jan 1;3:16-30.

[7] Aljumah A, Ahanger TA. Cyber security threats, challenges and defence mechanisms in cloud computing. IET communications. 2020 Apr;14(7):1185-91.

[8] Senk C. Adoption of security as a service. Journal of Internet Services and Applications. 2013 Dec;4:1-6.

[9] Sharma A, Keshwani B, Dadheech P. Authentication issues and techniques in cloud computing security: A review. InProceedings of International Conference on Sustainable Computing in Science, Technology and Management (SUSCOM), Amity University Rajasthan, Jaipur-India 2019 Feb 26.

[10] Gan Q, Wang X, Fang X. Efficient and secure auditing scheme for outsourced big data with dynamicity in cloud. Science China Information Sciences. 2018 Dec;61(12):122104.

[11] Liu W, Uluagac AS, Beyah R. MACA: A privacy-preserving multi-factor cloud authentication system utilizing big data. In2014 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS) 2014 Apr 27 (pp. 518-523). IEEE.

[12] Bhattasali T, Saeed K. Two factor remote authentication in healthcare. In2014 International Conference on Advances in Computing, Communications and Informatics (ICACCI) 2014 Sep 24 (pp. 380-386). IEEE.

[13] Castiglione A, De Santis A, Castiglione A, Palmieri F. An efficient and transparent one-time authentication protocol with non-interactive key scheduling and update. In2014 IEEE 28th International Conference on Advanced Information Networking and Applications 2014 May 13 (pp. 351-358). IEEE.

[14] Mahalakshmi B, Suseendran G. An analysis of cloud computing issues on data integrity, privacy and its current solutions. InData Management, Analytics and Innovation: Proceedings of ICDMAI 2018, Volume 2 2019 (pp. 467-482). Springer Singapore.

[15] Nandgaonkar SV, Raut AB. A comprehensive study on cloud computing. International Journal of Computer Science and Mobile Computing. 2014 Apr;3(4):733-8.

[16] Adee R, Mouratidis H. A dynamic four-step data security model for data in cloud computing based on cryptography and steganography. Sensors. 2022 Feb 1;22(3):1109.

[17] Thabit F, Alhomdy S, Al-Ahdal AH, Jagtap S. A new lightweight cryptographic algorithm for enhancing data security in cloud computing. Global Transitions Proceedings. 2021 Jun 1;2(1):91-9.

[18] Lee CK, Huo YZ, Zhang SZ, Ng KK. Design of a smart manufacturing system with the application of multi-access edge computing and blockchain technology. IEEE access. 2020 Feb 7;8:28659-67.