وزارت ارتباطات و فناوری اطلاعات
پژوهشگاه ارتباطات و فناوری اطلاعات

25.docx

بررسی روش‌های رصد خدمات ابری و ارزیابی بازار ابر ایران

عنوان گزارش: بررسی روش‌های رصد خدمات ابری و ارزیابی بازار ابر ایران

کلمات کلیدی: رصد خدمات ابری، بازار ابر، مبتنی‌بر دامنه، روش‌های استخراج شاخص‌ها

تهیه‌کنندگان: داود ملکی، نداء قربانی

ناظر علمی: دکتر احسان آریانیان، دکتر پژمان گودرزی، مهندس مریم محمودی

گروه پژوهشی سامانه‌های پردازش و تحلیل داده‌ها

سال انتشار: ۱۴۰۳

فهرست مطالب

۱- مقدمه

با گسترش سریع استفاده از فناوری‌های ابری، نیاز به رصد و پایش مداوم این زیرساخت‌ها به منظور تضمین عملکرد بهینه، امنیت و دسترس‌پذیری بیشتر احساس می‌شود. خدمات ابری به کاربران و سازمان‌ها این امکان را می‌دهد تا بدون نیاز به مدیریت مستقیم زیرساخت‌ها، به منابع پردازشی، ذخیره‌سازی و شبکه‌ای دسترسی داشته باشند. این ویژگی‌ها در عین حال که مزایای فراوانی دارند، چالش‌های جدیدی را نیز برای مدیریت و پایش این خدمات به همراه آورده‌اند.

مطابق مصوبه ۲۴۸ کمیسیون تنظیم مقررات – «شرایط شرایط و ضوابط صدور گواهینامه رتبه‌بندی و مجوز موقت مرکز داده»، سازمان فناوری اطلاعات ایران موظف است که مراکز داده و ارائه‌دهندگان خدمات ابری را رتبه‌بندی کند. این رتبه‌بندی نیاز به رصد مداوم کیفیت خدمات، امنیت و میزان رعایت استانداردها دارد. همچنانکه برای دریافت گواهینامه و مجوز موقت، ارائه‌دهندگان خدمات ابری باید استانداردهای مشخصی را رعایت کنند. رصد عملکرد این ارائه‌دهندگان و بررسی میزان تطابق آن‌ها با الزامات مصوبه ۲۴۷، بخشی از فرآیند نظارت بر خدمات ابری است. یکی از اهداف این مصوبه، افزایش سطح امنیت و قابلیت اطمینان مراکز داده و خدمات ابری است. این امر نیازمند ایجاد سامانه‌های رصد و پایش خدمات ابری به‌صورت مستمر است تا تخلفات، ضعف‌های امنیتی و مشکلات احتمالی شناسایی و مدیریت شوند. در این مصوبه، سازمان فناوری اطلاعات ایران به‌عنوان متولی اصلی پایش، ارزیابی و رتبه‌بندی مراکز داده و ارائه‌دهندگان خدمات ابری تعیین شده است. این سازمان باید ابزارهای نظارتی مناسب برای ارزیابی و گزارش‌دهی وضعیت خدمات ابری را فراهم کند. بنابراین، رصد خدمات ابری یکی از الزامات اجرایی مصوبه ۲۴۷ است و بدون وجود یک سیستم نظارتی قوی، اجرای مفاد این مصوبه امکان‌پذیر نخواهد بود.

۲- رصد خدمات ابری

رصد خدمت ابری شامل ردیابی و مدیریت عملکرد، در دسترس بودن و سلامت کلی خدمات مبتنی‌بر ابر است. این شامل معیارهای نظارتی مانند زمان کار، زمان پاسخگویی، توان عملیاتی، نرخ خطا و استفاده از منابع است تا اطمینان حاصل شود که خدمات ابری استانداردهای عملکرد مورد نیاز و قراردادهای سطح خدمت (SLA) را برآورده می‌کنند. نظارت مؤثر خدمت ابری به شناسایی مشکلات، بهینه‌سازی استفاده از منابع، بهبود امنیت و اطمینان از تجربه کاربری یکپارچه کمک می‌کند[۴]. رصد خدمات ابری به دلایل زیر ضروری است:

۱. **بهینه‌سازی عملکرد:** رصد خدمات به سازمان‌ها اجازه می‌دهد تا عملکرد خدمات ابری خود را ردیابی و بهینه کنند. با توجه به معیارهایی مانند زمان پاسخ و توان عملیاتی، شرکت‌ها می‌توانند از اجرای کارآمد خدمات خود اطمینان حاصل کنند. رصد خدمات به شناسایی تنگناهای عملکرد کمک می‌کند و مداخلات به موقع را برای افزایش عملکرد خدمات ممکن می‌کند [۵].
۲. **مدیریت هزینه:** رصد خدمات ابری مؤثر به مدیریت و بهینه‌سازی هزینه‌ها کمک می‌کند. با ردیابی استفاده از منابع، سازمان‌ها می‌توانند از تأمین بیش‌ازحد یا کمبود منابع جلوگیری کنند. رصد خدمات ابری می‌تواند منابع کم استفاده را نشان دهد و با اجازه دادن به سازمان‌ها برای کاهش مقیاس خدمات غیر ضروری منجر به صرفه‌جویی در هزینه‌ها شود[۶].
۳. **امنیت و انطباق:** رصد خدمات ابری برای حفظ امنیت و انطباق بسیار مهم است. رصد مستمر خدمات ابری می‌تواند فعالیت‌های غیرمعمول یا نقض‌های امنیتی احتمالی را شناسایی کند و امکان اقدام سریع برای کاهش خطرات را فراهم کند. خدمات ابری آمازون بر اهمیت رصد برای انطباق با استانداردها و مقررات صنعت تأکید می‌کند که می‌تواند از تخلفات پرهزینه و نقض داده‌ها جلوگیری کند.

۴. **قابلیت اطمینان و در دسترس بودن:** قابلیت اطمینان و در دسترس بودن خدمات ابری برای حفظ اعتماد و رضایت کاربر بسیار مهم است. ابزارهای رصد خدمات ابری می‌توانند تیم‌ها را در مورد مسائل، قبل از تأثیرگذاری بر کاربران آگاه کنند و تعمیر و نگهداری پیشگیرانه را تسهیل کنند. رصد زمان کار و نرخ خطا، به حفظ در دسترس بودن بالا و به حداقل رساندن زمان خرابی کمک می‌کند که برای مشاغلی که به خدمات ابری متکی هستند بسیار مهم است.

۵. **تجربه کاربر:** رصد مستقیماً با اطمینان از پاسخگو بودن و قابل اعتماد بودن خدمات، بر تجربه کاربر نهایی تأثیر می‌گذارد. ردیابی معیارهای تجربه کاربر به شناسایی و حل مشکلاتی که می‌تواند کیفیت خدمات را کاهش دهد کمک می‌کند. سولار ویندز[۱] تأکید می‌کند که حفظ تجربه کاربری مثبت از طریق نظارت می‌تواند منجر به رضایت مشتری و نرخ حفظ بالاتر شود[۷].

۲-۱- شاخص‌های کلیدی برای رصد خدمات ابری

شاخص‌های کلیدی رصد (KPI) برای خدمات ابری به متغیرهایی اشاره دارد که به کمک آن‌ها می‌توان عملکرد، امنیت و دسترس‌پذیری خدمات را سنجید. این شاخص‌ها به تیم‌های عملیاتی و مدیران فناوری اطلاعات کمک می‌کند تا وضعیت فعلی سامانه را ارزیابی کرده و تصمیمات آگاهانه‌تری اتخاذ کنند.

شاخص‌های عملکردی[۲]:

- استفاده از CPU: میزان استفاده از واحد پردازش مرکزی (CPU) یکی از مهم‌ترین شاخص‌ها برای ارزیابی بار کاری سرورها و کارایی اپلیکیشن‌ها است.
- استفاده از حافظه: این شاخص نشان‌دهنده میزان استفاده از حافظه (RAM) و منابع ذخیره‌سازی است که برای جلوگیری از کندی عملکرد یا خرابی سامانه‌ها اهمیت دارد.
- Disk I/O: سرعت و تعداد عملیات خواندن و نوشتن بر روی دیسک، یکی دیگر از شاخص‌های مهم است که می‌تواند تأثیر زیادی بر عملکرد اپلیکیشن‌ها داشته باشد.

شاخص‌های شبکه[۳]:

- تأخیر شبکه[۴]: تأخیر زمانی بین ارسال درخواست و دریافت پاسخ از سرویس، می‌تواند تأثیر مستقیم بر تجربه کاربر نهایی داشته باشد.
- پهنای باند[۵]: میزان داده‌هایی که در یک بازه زمانی مشخص از طریق شبکه انتقال می‌یابد، از اهمیت بالایی برخوردار است.
- نرخ از دست دادن بسته‌ها[۶]: از دست رفتن بسته‌های داده در حین انتقال می‌تواند نشانه‌ای از مشکلات شبکه یا ازدحام باشد.

---

[۱] SolarWinds
[۲] Performance Metrics
[۳] Network Metrics
[۴] Latency
[۵] Bandwidth
[۶] Packet Loss

شاخص‌های امنیتی[۱]:

- تعداد تلاش‌های ناموفق برای ورود: این شاخص می‌تواند نشان‌دهنده تلاش‌های ناموفق برای دسترسی غیرمجاز به سامانه‌ها باشد.
- فعالیت‌های غیرمعمول در فایروال: مشاهده هرگونه فعالیت مشکوک یا ترافیک غیرمجاز که از طریق فایروال رد یا مجاز شده است.
- تشخیص تهدیدها: تعداد تهدیدهای امنیتی شناسایی شده توسط سامانه‌های تشخیص نفوذ یا سایر ابزارهای امنیتی[۱, ۲].

معیارهای انتخاب روش مناسب رصد خدمات ابری:

- نوع خدمات ابری: بسته به نوع خدمات ابری (IaaS، PaaS، SaaS)، ممکن است روش‌های خاصی برای رصد مناسب‌تر باشند.
- مقیاس زیرساخت: سازمان‌های بزرگ‌تر با زیرساخت‌های پیچیده‌تر ممکن است نیاز به روش‌های پیشرفته‌تری داشته باشند.
- نیازهای امنیتی: برخی سازمان‌ها با توجه به حساسیت داده‌ها و اهمیت امنیت، نیاز به روش‌های رصد دقیق‌تری دارند[۳].

در این پژوهش به بررسی روش‌های استخراج شاخص‌های رصد خدمات ابری در لایه‌های IaaS، PaaS و SaaS پرداخته‌ایم. با توجه به ویژگی هر روش و شاخص‌های استخراج و دو شاخص دقت داده‌ها و زمان پاسخ در هر لایه از خدمات، یک رویکرد ترکیبی از روش‌های استخراج موجود ارائه کرده‌ایم.

۳- روش استخراج شاخص‌های رصد خدمات ابری

استخراج شاخص‌های لازم برای نظارت بر خدمات ابری را می‌توان از چند روش انجام داد. هر روش بسته به نوع خدمات ابری، عمق نظارت مورد نیاز و شاخص‌های خاصی که باید ردیابی شوند، شامل تکنیک‌ها و ابزارهای مختلفی است. در اینجا چند روش رایج وجود دارد:

۳-۱- روش‌های مبتنی‌بر عامل

یکی از روش‌های رایج برای استخراج شاخص‌های رصد خدمات ابری، استفاده از نرم‌افزارهای عامل[۲] است که به طور مستقیم بر روی سرورها، ماشین‌های مجازی یا کانتینرها نصب می‌شوند. این نرم‌افزارها اطلاعات دقیقی درباره وضعیت سامانه، استفاده از منابع و عملکرد اپلیکیشن‌ها جمع‌آوری می‌کنند.

عامل‌ها نرم‌افزارهای کوچکی هستند که به‌طور مستقل در یک سامانه ابری فعالیت می‌کنند و وظایف خاصی را اجرا می‌کنند. این عامل‌ها می‌توانند در نقاط مختلف شبکه، سرورها، ماشین‌های مجازی و یا حتی در خود خدمات نرم‌افزاری مستقر شوند. وظیفه اصلی آن‌ها نظارت بر سامانه، جمع‌آوری داده‌ها و ارائه گزارش‌های مربوط به عملکرد، امنیت و کیفیت خدمات است.

روش‌های مبتنی‌بر عامل به‌طورکلی از مدل‌های مختلفی برای مدیریت و پردازش داده‌های نظارتی استفاده می‌کنند. در اینجا به برخی از مدل‌های رایج اشاره می‌کنیم:

الف) عامل‌های توزیع‌شده[۳]: این مدل شامل استفاده از چندین عامل در نقاط مختلف زیرساخت ابری است. هر عامل وظیفه نظارت

---

[۱] Security Metrics
[۲] Agent
[۳] Distributed Agents

بر بخشی از خدمات یا زیرساخت را بر عهده دارد. این عامل‌ها داده‌ها را به‌صورت محلی جمع‌آوری و سپس به یک سرور مرکزی یا هماهنگ‌کننده ارسال می‌کنند. این روش باعث کاهش بار بر روی یک نقطه واحد می‌شود و انعطاف‌پذیری بالایی دارد.

ب) عامل‌های مستقل[۱]: در این روش، عامل‌ها به‌صورت خودمختار عمل می‌کنند و نیازی به دخالت دستی یا هماهنگ‌کننده مرکزی ندارند. آن‌ها قادر به تحلیل و تفسیر داده‌ها به‌صورت محلی هستند و می‌توانند در صورت نیاز تصمیم‌های خودکار نیز اتخاذ کنند. برای مثال، اگر یک عامل متوجه شود که میزان استفاده از منابع از یک حد بحرانی فراتر رفته است، می‌تواند اقدام به افزایش منابع کند.

ج) عامل‌های موبایل[۲]: این عامل‌ها می‌توانند از یک گره به گره دیگر در شبکه ابری حرکت کنند و داده‌ها را از نقاط مختلف جمع‌آوری کنند. این روش به‌ویژه در مواردی که نیاز به جمع‌آوری داده از بخش‌های مختلف و غیرمتمرکز سامانه است، کارایی دارد.

عامل‌های مبتنی‌بر رصد خدمات ابری قادر به جمع‌آوری انواع مختلفی از داده‌ها هستند که به تحلیل عملکرد، امنیت و کیفیت خدمات کمک می‌کنند:

الف) داده‌های عملکردی[۳]: این داده‌ها شامل اطلاعاتی مانند زمان پاسخگویی، زمان اجرای فرآیندها و میزان استفاده از منابع محاسباتی است که به بهبود کارایی خدمات کمک می‌کند.

ب) داده‌های امنیتی[۴]: عامل‌ها می‌توانند داده‌های مربوط به حملات سایبری، نقاط ضعف امنیتی، دسترسی‌های غیرمجاز و ورودهای ناموفق را جمع‌آوری کنند و به تحلیل و جلوگیری از تهدیدات امنیتی کمک کنند.

ج) داده‌های کیفی[۵]: این داده‌ها شامل تجربه کاربری[۶]، رضایت مشتری و پایداری خدمات می‌شوند. برای مثال، داده‌هایی که از نظرسنجی‌های کاربر یا تحلیل رفتار کاربر جمع‌آوری می‌شوند، به شناسایی مشکلات احتمالی و بهبود کیفیت خدمات کمک می‌کنند.

- **ابزارهای موجود برای استفاده از روش مبتنی‌بر عامل:**
  - Prometheus Node Exporter: ابزاری قدرتمند برای جمع‌آوری داده‌های عملکردی از سامانه‌ها که به صورت گسترده در محیط‌های ابری و کانتینری استفاده می‌شود.
  - Datadog Agent: این ابزار می‌تواند به طور یکپارچه داده‌ها را از منابع مختلف جمع‌آوری و تحلیل کند و به تیم‌های عملیاتی امکان دهد تا به سرعت مشکلات را شناسایی کنند.
- **مزایای استفاده از روش مبتنی‌بر عامل**
  - دسترسی به داده‌های دقیق: عامل‌ها می‌توانند اطلاعات بسیار دقیقی از وضعیت سامانه‌ها و منابع جمع‌آوری کنند.
  - بی‌درنگ: داده‌های جمع‌آوری شده توسط عامل‌ها به طور معمول به صورت بی‌درنگ[۷] در دسترس هستند.
- **معایب استفاده از روش مبتنی عامل**
  - افزایش بار کاری: نصب عامل‌ها ممکن است باعث افزایش بار کاری روی سرورها و کاهش عملکرد آن‌ها شود.
  - مسائل امنیتی: وجود عامل‌ها می‌تواند به عنوان یک نقطه‌ضعف امنیتی مورد سوءاستفاده قرار گیرد، به ویژه اگر به‌درستی پیکربندی نشده باشند[۸, ۹].

---

[۱] Autonomous Agents
[۲] Mobile Agents
[۳] Performance Metrics
[۴] Security Metrics
[۵] Quality Metrics
[۶] User Experience
[۷] Real-time

۳-۲- روش‌های مبتنی‌بر API

روش‌های مبتنی‌بر API به مدیران فناوری اطلاعات امکان می‌دهد تا بدون نیاز به نصب نرم‌افزارهای اضافی، داده‌های مورد نیاز خود را از خدمات ابری استخراج کنند. این روش‌ها از APIهای ارائه شده توسط سرویس‌دهندگان ابری برای جمع‌آوری اطلاعات استفاده می‌کنند.

استفاده از API ها در نظارت بر خدمات ابری به این معناست که مدیران سامانه و توسعه‌دهندگان می‌توانند از API های ارائه شده توسط ارائه‌دهندگان خدمات ابری برای دریافت داده‌های بی‌درنگ و تجزیه‌وتحلیل آن‌ها استفاده کنند. به‌این‌ترتیب، API ها نقش کلیدی در خودکارسازی فرآیند نظارت و مدیریت منابع ابری ایفا می‌کنند.

روش‌های استخراج مبتنی‌بر API در رصد خدمات ابری به چندین دسته تقسیم می‌شوند. این روش‌ها از طریق درخواست‌های API انجام می‌شود که از منابع مختلف خدمات ابری داده‌های مربوط به عملکرد و کارایی سامانه را استخراج می‌کنند. در ادامه به توضیح این روش‌ها پرداخته می‌شود:

الف) استخراج شاخص‌های عملکردی[۱]: یکی از اصلی‌ترین روش‌ها برای استخراج شاخص‌های رصد خدمات ابری استفاده از API های مربوط به عملکرد خدمات است. این شاخص‌ها شامل اطلاعاتی درباره استفاده از منابع محاسباتی، زمان پاسخگویی و توان عملیاتی سامانه‌ها هستند. ازجمله API هایی که برای این منظور استفاده می‌شوند عبارت‌اند از:

- API های استفاده از منابع: برای رصد استفاده از پردازنده (CPU)، حافظه (RAM) و فضای ذخیره‌سازی.
- API های شبکه: برای رصد پهنای باند، تأخیر[۲] و میزان دریافت و ارسال داده‌ها.
- API های کارایی ماشین‌های مجازی و کانتینرها: اطلاعات مربوط به وضعیت عملکرد ماشین‌های مجازی، کانتینرها و خدمات در حال اجرا را ارائه می‌دهند.

ب) استخراج شاخص‌های دسترسی و پایداری[۳]: شاخص‌های مربوط به پایداری خدمات و زمان دسترسی بسیار مهم هستند و API ها می‌توانند برای پایش این شاخص‌ها به کار روند. ازجمله این شاخص‌ها عبارت‌اند از:

- زمان آپ‌تایم (Uptime): مدت زمانی که خدمات بدون وقفه کار می‌کند.
- زمان در دسترس نبودن سامانه[۴]: مدت زمانی که خدمات در دسترس نیست یا با خطا مواجه است.
- API های تشخیص رخدادها: برای ثبت رخدادهای مختلف ازجمله قطع خدمات، خرابی سرورها و کاهش عملکرد.

API های مربوط به این بخش می‌توانند اطلاعات مربوط به وضعیت دسترسی به خدمات را جمع‌آوری کرده و به تحلیل این شاخص‌ها کمک کنند.

ج) استخراج شاخص‌های امنیتی: یکی دیگر از روش‌های مهم استخراج شاخص‌ها از طریق API، نظارت بر جنبه‌های امنیتی خدمات ابری است. API های امنیتی برای رصد کردن دسترسی‌های غیرمجاز، شناسایی رفتارهای مشکوک و حفظ داده‌ها به کار می‌روند.

- API های مدیریت هویت و دسترسی (IAM APIs): این API ها برای نظارت بر دسترسی کاربران و مدیریت مجوزهای امنیتی استفاده می‌شوند.

---

۱ Performance Monitoring
۲ Latency
۳ Availability and Reliability Monitoring
۴ Downtime

- API های تشخیص حملات[۱]: این API ها به شناسایی و پاسخگویی به حملات سایبری مانندDDOS[۲] و سایر تهدیدات امنیتی کمک می‌کنند.

د) استخراج شاخص‌های تجربه کاربر[۳]: API های مرتبط با تجربه کاربری به ما کمک می‌کنند که عملکرد و کیفیت خدمات را از دید کاربران نهایی ارزیابی کنیم. این شاخص‌ها شامل مواردی مانند زمان بارگذاری صفحات وب، تأخیر در پاسخگویی خدمات و دیگر عواملی است که بر تجربه کاربر تأثیر می‌گذارد.

- API های زمان پاسخگویی: برای اندازه‌گیری زمان پاسخ به درخواست‌های کاربر.
- API های کیفیت خدمات (QoS APIs): این API ها شاخص‌های مربوط به کیفیت کلی خدمات از دید کاربر نهایی را استخراج می‌کنند.

- **مراحل استخراج شاخص‌ها با API**

۱. **ثبت‌نام و دسترسی به API:** اولین گام دریافت دسترسی به API های ارائه‌دهندگان ابری است. این کار معمولاً شامل ثبت‌نام در پلتفرم ابری و دریافت کلیدهای API (API Keys) است.

۲. **ارسال درخواست‌ها:** پس از دریافت کلید API، درخواست‌های HTTP/HTTPS به سرورهای API ارسال می‌شود. این درخواست‌ها ممکن است شامل درخواست‌های GET (برای دریافت داده‌ها)، POST (برای ارسال داده‌ها) و PUT (برای به‌روزرسانی داده‌ها) باشند.

۳. **دریافت پاسخ:** سرور API در پاسخ به درخواست‌های ارسالی، داده‌های مربوط به شاخص‌های رصد را به‌صورت ساختاریافته (اغلب در قالب JSON یا XML) ارسال می‌کند.

۴. **پردازش و تجزیه‌وتحلیل داده‌ها:** داده‌های دریافتی از API به‌وسیله ابزارهای تحلیلی یا اسکریپت‌های نوشته شده توسط تیم فنی پردازش و تحلیل می‌شوند تا شاخص‌های عملکرد، دسترسی، امنیت و کیفیت استخراج و بررسی شوند.

۵. **گزارش‌گیری و نمایش شاخص‌ها:** در نهایت، داده‌ها به‌صورت نمودارها و گزارش‌های بی‌درنگ به تیم مدیریت ارائه می‌شود. این گزارش‌ها به تصمیم‌گیری‌های راهبردی درباره بهبود عملکرد و افزایش کارایی خدمات ابری کمک می‌کنند.

- **مزایای استفاده از روش‌های مبتنی‌بر API**

- عدم نیاز به نصب نرم‌افزارهای اضافی: این روش نیاز به نصب عامل‌ها را حذف می‌کند و از APIهای موجود برای جمع‌آوری داده‌ها استفاده می‌کند.
- مقیاس‌پذیری: این روش به راحتی قابل مقیاس‌بندی است و می‌تواند در محیط‌های بزرگ به کار رود.

- **معایب استفاده از روش‌های مبتنی‌بر API**

- محدودیت‌های API: استفاده از این روش‌ها به میزان داده‌ها و شاخص‌هایی که APIهای سرویس‌دهنده ارائه می‌دهند، محدود است.
- هزینه‌ها: در برخی موارد، استفاده مکرر از APIها می‌تواند هزینه‌های اضافی ایجاد کند، به ویژه در صورت نیاز به داده‌های بی‌درنگ.

---

[۱] Intrusion Detection APIs
[۲] Distributed Denial-of-Service
[۳] User Experience Monitoring

۳-۳- روش‌های مبتنی‌بر لاگ

لاگ‌ها، فایل‌ها یا جریان‌هایی از داده‌ها هستند که شامل اطلاعات مربوط به فعالیت‌ها، خطاها، درخواست‌ها و پاسخ‌ها، تغییرات در تنظیمات و دیگر جزئیات مربوط به عملیات خدمات ابری می‌باشند. هر سامانه ابری (مانند زیرساخت ابری، پایگاه داده‌ها، ماشین‌های مجازی و کانتینرها) به‌طور مداوم لاگ‌هایی تولید می‌کند که می‌توانند برای تحلیل و نظارت استفاده شود. لاگ‌ها شامل سوابق دقیق از رخدادها و عملیات‌های مختلف در سامانه‌ها و خدمات ابری هستند. جمع‌آوری و تحلیل لاگ‌ها می‌تواند اطلاعات ارزشمندی درباره مشکلات سامانه، امنیت و عملکرد ارائه دهد.

استخراج شاخص‌های رصد مبتنی‌بر لاگ به معنی جمع‌آوری، پردازش و تجزیه‌وتحلیل لاگ‌ها با هدف دستیابی به اطلاعات کلیدی درباره عملکرد و سلامت خدمات ابری است. برخی از روش‌های رایج در این زمینه عبارت‌اند از:

الف) جمع‌آوری لاگ‌ها[۱]: اولین مرحله در استخراج شاخص‌های رصد خدمات ابری، جمع‌آوری لاگ‌ها از منابع مختلف ابری است. لاگ‌ها ممکن است از اجزای مختلف زیرساخت ابری مانند سرورها، ماشین‌های مجازی، کانتینرها، پایگاه‌داده‌ها، فایروال‌ها و سایر سامانه‌های مرتبط تولید شوند. ابزارهای مختلفی برای جمع‌آوری لاگ‌ها وجود دارند که معمولاً به‌صورت خودکار لاگ‌ها را از منابع مختلف استخراج کرده و در یک پایگاه داده مرکزی یا خدمات لاگ‌محور ذخیره می‌کنند.

ب) ذخیره‌سازی و مدیریت لاگ‌ها[۲]: پس از جمع‌آوری لاگ‌ها، باید این اطلاعات در یک مخزن مرکزی ذخیره و مدیریت شوند. این کار به‌طورمعمول توسط ابزارهایی مانند پایگاه‌های داده لاگ‌محور انجام می‌شود. سامانه‌های ذخیره‌سازی لاگ باید قادر به نگهداری حجم عظیمی از داده‌ها به‌صورت بهینه و مقیاس‌پذیر باشند، زیرا سامانه‌های ابری می‌توانند حجم بالایی از لاگ‌ها تولید کنند.

ج) تحلیل و تجزیه لاگ‌ها[۳]: در این مرحله، لاگ‌ها بر اساس نوع و ساختارشان تجزیه‌وتحلیل می‌شوند. لاگ‌ها به‌صورت خام ممکن است شامل اطلاعات بسیاری باشند که باید فیلتر شده و تنها اطلاعات مفید استخراج شود. تحلیل لاگ‌ها معمولاً شامل شناسایی الگوها، استخراج رخدادهای مهم، شناسایی خطاها و مسائل عملکردی و همچنین محاسبه شاخص‌های کلیدی عملکرد است.

د) بصری‌سازی و گزارش‌گیری[۴]: پس از تحلیل لاگ‌ها، نتایج به‌صورت گراف‌ها و گزارش‌های مختلف به تیم‌های مدیریتی و فنی ارائه می‌شود. ابزارهای بصری‌سازی لاگ‌ها می‌توانند روندها و الگوهای موجود در داده‌ها را نمایش دهند و به تیم‌ها کمک کنند که مسائل را سریع‌تر شناسایی و رفع کنند.

- **فرآیندهای تحلیل برای روش‌های مبتنی‌بر لاگ**
  - فیلتر کردن لاگ‌ها: حذف داده‌های غیرضروری و تمرکز روی رخدادهای مهم مانند خطاها یا درخواست‌های ناموفق.
  - استخراج رخدادها: شناسایی رخدادهای مهم مثل خرابی‌ها، کاهش عملکرد یا حملات امنیتی.
  - تجمیع داده‌ها: ترکیب اطلاعات از لاگ‌های مختلف برای ایجاد بینش کلی از وضعیت سامانه.
- **انواع لاگ‌های مورداستفاده در نظارت بر خدمات ابری**

الف) لاگ‌های سامانه[۵]: این لاگ‌ها شامل اطلاعات مربوط به عملکرد کلی سامانه‌های ابری هستند؛ مانند وضعیت ماشین‌های مجازی، کانتینرها، سرورها و منابع محاسباتی.

---

۱ Log Collection
۲ Log Storage and Management
۳ Log Parsing and Analysis
۴ Visualization and Reporting
۵ System Logs

- شاخص‌های استخراج‌شده،
- استفاده از منابع مانند CPU، حافظه و دیسک.
- وضعیت شبکه و میزان پهنای باند مصرف‌شده.
- وضعیت راه‌اندازی یا خاموشی ماشین‌ها و خدمات

ب) لاگ‌های اپلیکیشن[۱]: این نوع لاگ‌ها شامل داده‌های مربوط به اجرای اپلیکیشن‌ها و خدمات مبتنی‌بر ابر هستند. اطلاعات لاگ‌های اپلیکیشن می‌تواند مشخص کند که آیا اپلیکیشن با موفقیت اجرا شده یا با خطا مواجه شده است.

- شاخص‌های استخراج‌شده
- زمان پاسخگویی اپلیکیشن
- تعداد درخواست‌های موفق و ناموفق
- خطاهای رخ‌داده در اجرای اپلیکیشن

ج) لاگ‌های امنیتی: این لاگ‌ها شامل اطلاعاتی درباره رخدادهای امنیتی، دسترسی‌ها، تغییرات پیکربندی و تلاش‌های غیرمجاز برای ورود به سامانه‌ها هستند. از لاگ‌های امنیتی می‌توان برای شناسایی حملات سایبری، رخدادهای مشکوک و آسیب‌پذیری‌های امنیتی استفاده کرد.

- شاخص‌های استخراج‌شده.
- تعداد و نوع حملات شناسایی‌شده.
- تلاش‌های ناموفق برای ورود به سامانه.
- تغییرات مشکوک در پیکربندی‌ها یا دسترسی‌ها.

د) لاگ‌های شبکه[۲]: این لاگ‌ها شامل اطلاعاتی درباره ترافیک شبکه، بسته‌های ارسال و دریافت‌شده، تأخیر شبکه و مسائل مربوط به پهنای باند هستند.

- شاخص‌های استخراج‌شده.
- میزان ترافیک ورودی و خروجی.
- تأخیر شبکه و میزان از دست رفتن بسته‌ها.
- میزان استفاده از پهنای باند.

○ مراحل اجرای روش‌های استخراج لاگ‌ها در رصد خدمات ابری

الف) پیکربندی و جمع‌آوری لاگ‌ها: در این مرحله باید منابع ابری خود را به‌گونه‌ای پیکربندی نمود که لاگ‌ها به‌صورت خودکار به یک مخزن مرکزی ارسال شوند. ابزارهای مدیریت لاگ مانند CloudWatch، Stackdriver یا Elastic Stack معمولاً برای این منظور استفاده می‌شوند.

ب) پردازش و تجزیه‌وتحلیل لاگ‌ها: پس از جمع‌آوری لاگ‌ها، ابزارهای تحلیل لاگ باید به‌طور خودکار داده‌ها را پردازش کرده و شاخص‌های کلیدی عملکرد را استخراج کنند. این مرحله ممکن است شامل شناسایی الگوها، رخدادهای غیرمعمول و محاسبه شاخص‌هایی مانند میانگین زمان پاسخگویی یا تعداد خطاها باشد.

---

[۱] Application Logs
[۲] Network Logs

ج) ایجاد گزارش و داشبوردها: نتایج تجزیه‌وتحلیل لاگ‌ها باید به‌صورت داشبوردها و گزارش‌های بصری در اختیار مدیران و تیم‌های فنی قرار گیرد تا بتوانند از وضعیت سامانه‌ها و خدمات ابری خودآگاهی پیدا کنند.

- **ابزارها و خدمات جمع‌آوری و تحلیل لاگ‌ها**

- ELK Stack[۱]: یک مجموعه از ابزارهای قدرتمند برای جمع‌آوری، تجزیه‌وتحلیل و بصری‌سازی لاگ‌ها که به طور گسترده در محیط‌های ابری و سازمانی استفاده می‌شود.
- Splunk: ابزاری قدرتمند برای جمع‌آوری و تحلیل لاگ‌ها که به تیم‌های امنیتی و عملیاتی امکان می‌دهد تا به سرعت مشکلات را شناسایی و رفع کنند.

- **مزایای استفاده از روش‌های مبتنی‌بر لاگ**

- جزئیات بالا: لاگ‌ها اطلاعات بسیار دقیقی از رخدادها و عملیات‌های سامانه ارائه می‌دهند که می‌تواند به شناسایی دقیق مشکلات کمک کند.
- تاریخچه قابل جستجو: لاگ‌ها به مدیران اجازه می‌دهند تا تاریخچه‌ای از رخدادها را بررسی کرده و الگوهای غیرعادی را شناسایی کنند.

- **معایب استفاده از روش‌های مبتنی‌بر لاگ**

- حجم بالای داده‌ها: جمع‌آوری و ذخیره لاگ‌ها می‌تواند به حجم بسیار بالایی از داده‌ها منجر شود که نیاز به فضای ذخیره‌سازی و منابع پردازشی زیاد دارد.
- تأخیر در پردازش: بسته به حجم داده‌ها، ممکن است تحلیل لاگ‌ها زمان‌بر باشد و نتواند بی‌درنگ انجام شود.

۳-۴- روش‌های مبتنی‌بر ترافیک شبکه

یکی دیگر از روش‌های مؤثر برای رصد خدمات ابری، روش‌های استخراج ترافیک شبکه است. این روش به بررسی و تحلیل جریان داده‌ها در شبکه می‌پردازد و می‌تواند اطلاعاتی نظیر پهنای باند مصرفی، تأخیر شبکه و نرخ از دست رفتن بسته‌ها را ارائه دهد.

ترافیک شبکه شامل داده‌هایی است که بین خدمات ابری و کاربران یا میان خدمات مختلف در یک محیط ابری جابه‌جا می‌شوند. این داده‌ها می‌توانند شامل درخواست‌های کاربران، پاسخ‌های سرورها، تبادل داده‌ها بین ماشین‌های مجازی و کانتینرها و بسیاری دیگر از تعاملات شبکه‌ای باشند. رصد ترافیک شبکه از این نظر اهمیت دارد که می‌تواند اطلاعات ارزشمندی در مورد عملکرد، امنیت و کیفیت خدمات ابری ارائه دهد.

روش‌های مختلفی برای استخراج شاخص‌های کلیدی عملکرد (KPIs) از ترافیک شبکه وجود دارد که هر یک به ابعاد مختلفی از عملکرد و وضعیت شبکه متمرکز هستند. این روش‌ها شامل تحلیل داده‌های شبکه، تشخیص مشکلات عملکردی و شناسایی تهدیدات امنیتی است.

الف) جمع‌آوری داده‌های ترافیک شبکه[۲]: اولین گام برای استخراج شاخص‌های شبکه، جمع‌آوری داده‌های ترافیک است. داده‌های ترافیک می‌توانند شامل بسته‌های شبکه، جریان‌های داده[۳] و دیگر اطلاعات مرتبط با تعاملات شبکه‌ای باشند. برای جمع‌آوری این داده‌ها

---

[۱] Elasticsearch, Logstash, Kibana
[۲] Network Traffic Data Collection
[۳] Flows

معمولاً از ابزارهای نظارت بر شبکه استفاده می‌شود.

ابزارهای رایج برای جمع‌آوری ترافیک شبکه:

- Wireshark: ابزاری منبع‌باز برای بررسی و تحلیل بسته‌های شبکه.
- NetFlow: پروتکل شبکه‌ای که برای جمع‌آوری و پایش اطلاعات جریان‌های داده در شبکه استفاده می‌شود.
- sFlow: ابزار دیگری برای جمع‌آوری نمونه‌های داده‌های شبکه که به صورت بی‌درنگ ترافیک شبکه را پایش می‌کند.
- Cloud-native tools: مانند VPC Flow Logs در AWS و Google Cloud VPC Flow Logs برای پایش ترافیک در خدمات ابری.

ب) تحلیل و تجزیه داده‌های ترافیک[۱]**:** پس از جمع‌آوری داده‌های ترافیک، این اطلاعات باید تحلیل و پردازش شوند تا شاخص‌های کلیدی عملکرد (KPI) استخراج شوند. تحلیل ترافیک شبکه به شناسایی الگوها، رخدادهای غیرمعمول و مسائل عملکردی مانند تأخیر بالا یا کاهش پهنای باند کمک می‌کند.

انواع تحلیل‌ها:

- تحلیل بسته‌ها[۲]: شامل تجزیه‌وتحلیل هر بسته داده است که در شبکه منتقل می‌شود. این تحلیل می‌تواند اطلاعات دقیقی از پروتکل‌های شبکه، اندازه بسته‌ها و زمان انتقال آن‌ها ارائه دهد.
- تحلیل جریان‌ها[۳]: جریان‌های داده‌ای که بین خدمات منتقل می‌شوند، به‌ویژه در خدمات ابری که از چندین نقطه جغرافیایی استفاده می‌کنند، مورد تحلیل قرار می‌گیرند. این تحلیل برای فهمیدن الگوی انتقال داده‌ها و مشکلات احتمالی مانند گلوگاه‌ها مفید است.

ج) شاخص‌های کلیدی عملکرد شبکه (KPIs): از طریق جمع‌آوری و تحلیل داده‌های ترافیک شبکه، می‌توان شاخص‌های کلیدی مختلفی را برای ارزیابی عملکرد شبکه در خدمات ابری استخراج کرد. برخی از شاخص‌های مهم عبارت‌اند از:

۱. **پهنای باند**[۴]**:** میزان داده‌ای که در واحد زمان از شبکه عبور می‌کند. این شاخص نشان‌دهنده ظرفیت شبکه و میزان استفاده از منابع شبکه‌ای است. کاهش پهنای باند می‌تواند به معنی ازدحام شبکه یا مشکلات زیرساختی باشد.

۲. تأخیر شبکه: مدت زمانی که طول می‌کشد تا یک بسته داده از مبدأ به مقصد برسد. تأخیر بالا می‌تواند نشان‌دهنده مشکلاتی در مسیرهای شبکه، ازدحام یا تنظیمات نادرست باشد.

۳. **اتلاف بسته‌ها**[۵]**:** درصد بسته‌های داده که در طول انتقال از شبکه از دست می‌روند. اتلاف بسته‌ها می‌تواند ناشی از مشکلات در مسیریاب‌ها، ازدحام شبکه یا مسائل امنیتی باشد.

۴. **زمان خرابی**[۶] **و دسترسی‌پذیری**[۷]**:** زمان دسترسی‌پذیری و پایداری خدمات ابری از طریق شبکه. کاهش آپ‌تایم یا دسترسی‌پذیری می‌تواند نشان‌دهنده قطعی شبکه یا مشکلات در سرورهای ابری باشد.

---

۱ Network Traffic Analysis
۲ Packet Analysis
۳ Flow Analysis
۴ Bandwidth
۵ Packet Loss
۶ Uptime
۷ Availability

۵. **تعداد درخواست‌های موفق و ناموفق**[۱]: این شاخص میزان موفقیت درخواست‌های شبکه‌ای را نشان می‌دهد. نرخ بالای درخواست‌های ناموفق می‌تواند ناشی از مشکلات در زیرساخت شبکه یا خطاهای امنیتی باشد.

۶. **میزان ازدحام**[۲]: ازدحام شبکه به میزان بار اضافی که روی شبکه قرار دارد و باعث کندی و افت کیفیت خدمات می‌شود، اشاره دارد. این شاخص به شناسایی نقاط گلوگاهی کمک می‌کند.

د) شناسایی رخدادهای غیرمعمول و مشکلات امنیتی[۳]: ترافیک شبکه می‌تواند به شناسایی تهدیدات امنیتی و رخدادهای غیرمعمول کمک کند. این نوع تحلیل به‌طور خاص برای شناسایی حملات سایبری، مثل حملات DDoS یا تلاش‌های غیرمجاز برای دسترسی به خدمات کاربرد دارد.

تحلیل‌های امنیتی:

- تشخیص الگوهای غیرعادی: مانند افزایش ناگهانی در ترافیک ورودی که ممکن است نشانه‌ای از یک حمله DDoS باشد.
- شناسایی ترافیک مشکوک: تحلیل لاگ‌های فایروال و سایر سامانه‌های امنیتی برای شناسایی ترافیک‌های غیرمجاز و مشکوک.

هـ) بصری‌سازی و گزارش‌گیری[۴]: در نهایت، داده‌های استخراج‌شده و تحلیل‌شده باید به‌صورت گزارش‌ها و داشبوردهای گرافیکی ارائه شوند. ابزارهای بصری‌سازی کمک می‌کنند تا تیم‌های فنی و مدیریتی بتوانند وضعیت شبکه را به‌سرعت بررسی کرده و اقدامات لازم را در صورت بروز مشکل انجام دهند.

- **مراحل اجرای روش‌های استخراج ترافیک شبکه در رصد خدمات ابری**

الف) پیکربندی و جمع‌آوری داده‌ها: ابتدا باید منابع شبکه‌ای و خدمات ابری خود را به‌گونه‌ای پیکربندی کنید که داده‌های ترافیک شبکه به‌صورت خودکار جمع‌آوری شود. استفاده از ابزارهایی مانند VPC Flow Logs یا NetFlow می‌تواند به جمع‌آوری اطلاعات ترافیک کمک کند.

ب) تحلیل و پردازش داده‌ها: پس از جمع‌آوری داده‌های ترافیک، ابزارهای تحلیل شبکه داده‌ها را پردازش و تحلیل می‌کنند. این مرحله شامل شناسایی الگوهای ترافیکی، محاسبه شاخص‌های عملکردی و تشخیص رخدادهای غیرعادی است.

ج) گزارش‌گیری و داشبوردها: نتایج تحلیل باید به‌صورت داشبوردهای بی‌درنگ و گزارش‌های جامع در اختیار تیم‌های مدیریتی و فنی قرار گیرد. این گزارش‌ها به شناسایی مشکلات شبکه، پیش‌بینی بحران‌ها و بهبود عملکرد خدمات ابری کمک می‌کنند.

ابزارهای روش‌های استخراج شبکه:

- Wireshark: یک ابزار رایگان و منبع باز برای تجزیه‌وتحلیل بسته‌های شبکه که به شناسایی مشکلات شبکه کمک می‌کند.
- NetFlow: پروتکل جمع‌آوری اطلاعات شبکه که توسط مسیریاب‌ها و سوییچ‌های سیسکو استفاده می‌شود و امکان تجزیه‌وتحلیل ترافیک شبکه را فراهم می‌کند.

- **مزایای استفاده از این روش‌های مبتنی‌بر شبکه**

- شناسایی مشکلات شبکه: این روش می‌تواند مشکلات مربوط به پهنای باند، تأخیر شبکه و ازدحام شبکه را شناسایی و رفع

---

[۱] Successful and Failed Requests
[۲] Congestion Level
[۳] Anomaly Detection and Security Monitoring
[۴] Visualization and Reporting

کند.

- بهبود امنیت شبکه: با روش‌های استخراج ترافیک شبکه، می‌توان فعالیت‌های غیرمجاز و تهدیدات امنیتی را شناسایی و از بروز حملات جلوگیری کرد.

- **معایب استفاده از روش‌های مبتنی‌بر شبکه**

- پیچیدگی پیاده‌سازی: روش‌های استخراج ترافیک شبکه نیاز به دانش فنی بالا و ابزارهای تخصصی دارد که ممکن است برای برخی سازمان‌ها چالش‌برانگیز باشد.
- نیاز به منابع زیاد: پردازش و تجزیه‌وتحلیل داده‌های شبکه به منابع پردازشی و ذخیره‌سازی زیادی نیاز دارد[۱۰].

۳-۵- روش‌های مبتنی‌بر تله‌متری

به جمع‌آوری و انتقال داده‌های عملکردی از خدمات و اپلیکیشن‌های ابری اشاره دارد که به صورت توزیع شده اجرا می‌شوند. این روش به خصوص در محیط‌های میکروسرویس بسیار کاربردی است و امکان ارائه یک دید کلی و جامع از وضعیت سامانه‌ها را فراهم می‌کند.

تله‌متری فرآیند خودکار جمع‌آوری، انتقال و تحلیل داده‌ها از منابع مختلف (مانند سرورها، شبکه‌ها، اپلیکیشن‌ها و دستگاه‌های فیزیکی) است. این داده‌ها معمولاً شامل اطلاعاتی درباره عملکرد، استفاده از منابع، خطاها و رخدادهای مختلف در سامانه‌های ابری هستند. در محیط‌های ابری، این داده‌ها از منابع مختلف مانند ماشین‌های مجازی، کانتینرها، پایگاه‌داده‌ها و شبکه‌ها جمع‌آوری می‌شوند.

استخراج شاخص‌های رصد از طریق تله‌متری شامل چندین مرحله است که به‌صورت پیوسته انجام می‌شوند. این مراحل عبارت‌اند از:

الف) جمع‌آوری داده‌های تله‌متری[۱]: اولین مرحله در فرآیند استخراج شاخص‌های رصد، جمع‌آوری داده‌های تله‌متری از منابع مختلف ابری است. این داده‌ها می‌توانند شامل اطلاعاتی مانند مصرف CPU، حافظه، پهنای باند، تأخیر در شبکه و رخدادهای خاص مانند خطاها و موفقیت‌ها در اجرای عملیات باشند.

ب) ذخیره‌سازی و مدیریت داده‌های تله‌متری[۲]: پس از جمع‌آوری داده‌های تله‌متری، این داده‌ها باید به‌طور مناسب ذخیره و مدیریت شوند. این داده‌ها به‌طورمعمول در سامانه‌های پایگاه داده‌های سری زمانی[۳] ذخیره می‌شوند. این سامانه‌ها داده‌ها را به ترتیب زمانی سازمان‌دهی می‌کنند و امکان تحلیل بهتر آن‌ها را فراهم می‌آورند.

ج) تحلیل و تجزیه داده‌های تله‌متری[۴]: در این مرحله، داده‌های جمع‌آوری‌شده تحلیل می‌شوند تا شاخص‌های کلیدی عملکرد (KPI) استخراج شوند. تحلیل تله‌متری معمولاً به دو روش انجام می‌شود:

- تحلیل بی‌درنگ: داده‌ها به‌صورت بی‌درنگ تحلیل می‌شوند تا مشکلات فوری شناسایی شوند.
- تحلیل تاریخی: داده‌های ذخیره‌شده به‌صورت تاریخی تحلیل می‌شوند تا روندها، الگوها و مشکلات تکراری شناسایی شوند.

شاخص‌های کلیدی استخراج‌شده از داده‌های تله‌متری:

۱. استفاده از CPU: نشان‌دهنده میزان مصرف پردازشگر توسط خدمات و منابع ابری است.
۲. استفاده از حافظه: مقدار حافظه‌ای که توسط خدمات مصرف می‌شود.
۳. پهنای باند شبکه: میزان داده‌هایی که از طریق شبکه منتقل می‌شود.

---

[۱] Telemetry Data Collection
[۲] Telemetry Data Storage and Management
[۳] Time-series Databases
[۴] Telemetry Data Analysis

۴. تأخیر شبکه: زمانی که طول می‌کشد تا درخواست‌ها به خدمات ابری برسند و پاسخ داده شوند.
۵. رخدادهای خطا: تعداد و نوع خطاهایی که در منابع ابری رخ داده است.

د) بصری‌سازی و گزارش‌گیری[۱]: داده‌های تله‌متری پس از تحلیل، باید به‌صورت بصری و قابل فهم ارائه شوند تا تیم‌های مدیریتی و فنی بتوانند از آن‌ها برای تصمیم‌گیری استفاده کنند. ابزارهای بصری‌سازی و گزارش‌گیری کمک می‌کنند تا شاخص‌های عملکردی به‌صورت گراف‌ها و داشبوردهای تعاملی نمایش داده شوند.

- **ابزارهای ذخیره‌سازی**
  - InfluxDB: پایگاه داده‌ای سری زمانی که برای ذخیره‌سازی و مدیریت داده‌های تله‌متری استفاده می‌شود.
  - OpenTSDB: یک پایگاه داده سری زمانی که معمولاً برای داده‌های بزرگ استفاده می‌شود.
  - Elasticsearch: ابزاری برای ذخیره‌سازی و جستجوی داده‌های تله‌متری و لاگ‌ها.
- **انواع داده‌های تله‌متری و شاخص‌های مرتبط**

الف) داده‌های زیرساخت: این نوع داده‌ها شامل اطلاعاتی از سطح زیرساخت ابری مانند ماشین‌های مجازی، کانتینرها و سرورها است. برخی از شاخص‌های مهم این دسته عبارت‌اند از:

- استفاده از منابع سخت‌افزاری (CPU، حافظه، دیسک): برای بررسی میزان استفاده و ظرفیت منابع.
- آپ‌تایم و زمان خرابی[۲]: برای ارزیابی پایداری زیرساخت.
- نرخ درخواست‌ها و پاسخ‌ها[۳]: برای ارزیابی کارایی زیرساخت.

ب) داده‌های شبکه [۴]: این داده‌ها شامل اطلاعاتی درباره ترافیک شبکه و ارتباطات بین منابع ابری است. شاخص‌های کلیدی این دسته شامل موارد زیر است:

- پهنای باند مصرفی[۵]: میزان داده‌هایی که از طریق شبکه منتقل می‌شود.
- تأخیر شبکه[۶]: مدت زمان لازم برای انتقال داده‌ها در شبکه.
- افت بسته‌ها[۷]: درصد بسته‌هایی که در طول انتقال از دست می‌روند.

ج) داده‌های اپلیکیشن تله‌متری: این نوع داده‌ها شامل اطلاعاتی درباره عملکرد اپلیکیشن‌ها و خدمات اجراشده در محیط ابری است. شاخص‌های کلیدی این دسته عبارت‌اند از:

- زمان پاسخگویی اپلیکیشن[۸]: مدت زمان لازم برای پردازش درخواست‌ها توسط اپلیکیشن.
- تعداد درخواست‌های موفق و ناموفق: شاخصی برای سنجش میزان موفقیت اپلیکیشن در پاسخگویی به درخواست‌ها.
- رخدادهای خطا و هشدارها: شناسایی رخدادهای خطا یا وضعیت‌های غیرعادی.

---

[۱] Visualization and Reporting
[۲] Uptime and Downtime
[۳] Request/Response Rate
[۴] Network Telemetry
[۵] Bandwidth Usage
[۶] Network Latency
[۷] Packet Loss
[۸] Application Response Time

- **ابزارهای تله‌متری**
  - Open Telemetry: پروژه‌ای منبع باز که به جمع‌آوری، پردازش و انتقال داده‌های تله‌متری از اپلیکیشن‌ها و خدمات ابری می‌پردازد.
  - Jaeger: ابزاری برای رصد و ردیابی درخواست‌ها در سامانه‌های توزیع شده که به شناسایی مشکلات عملکردی و بهینه‌سازی خدمات کمک می‌کند.
- **مزایای استفاده از روش‌های مبتنی‌بر تله‌متری**
  - دید کلی از سامانه‌ها: این روش به مدیران امکان می‌دهد تا وضعیت کلی خدمات و ارتباطات میان آن‌ها را به خوبی مشاهده کنند.
  - قابلیت مقیاس‌پذیری: این روش برای محیط‌های بزرگ و سامانه‌های توزیع شده مناسب است و می‌تواند با نیازهای مقیاس‌پذیری سازمان‌ها هماهنگ شود.
- **معایب استفاده از این روش‌های مبتنی‌بر تله‌متری**
  - پیچیدگی پیاده‌سازی: پیاده‌سازی و مدیریت تله‌متری در سامانه‌های توزیع شده نیاز به دانش تخصصی و ابزارهای پیشرفته دارد.
  - هزینه‌های اجرایی: جمع‌آوری و پردازش حجم بالای داده‌های تله‌متری می‌تواند هزینه‌بر باشد[۱۱].

۳-۶- روش‌های مبتنی‌بر رویداد

روش‌های مبتنی‌بر رویداد به تحلیل و پایش رویدادهای خاص در زیرساخت ابری می‌پردازند. این رویدادها می‌توانند شامل خرابی سرویس، افزایش ناگهانی ترافیک، یا تغییرات پیکربندی باشند.

رویدادها در واقع واحدهایی از اطلاعات هستند که نشان‌دهنده وقوع یک وضعیت یا تغییر خاص در خدمات ابری می‌باشند. به‌عنوان‌مثال:

- رویدادهای عملکردی: نشان‌دهنده عملیات‌هایی هستند که خدمات ابری برای کاربران انجام می‌دهند.
- رویدادهای امنیتی: رویدادهایی که به تغییرات در امنیت و دسترسی‌ها اشاره می‌کنند (مانند ورود کاربر، دسترسی‌های غیرمجاز).
- رویدادهای خطا: هرگونه خرابی، قطع ارتباط یا شکست در عملکرد خدمات که باید به آن‌ها توجه شود.

فرآیند استخراج شاخص‌های کلیدی عملکرد (KPIs) از رویدادهای ابری شامل چندین مرحله است که به شرح زیر توضیح داده شده‌اند:

الف) جمع‌آوری رویدادها[۱]: در مرحله اول، رویدادهای تولید شده در سامانه‌های ابری باید به‌صورت مداوم و خودکار جمع‌آوری شوند. این رویدادها می‌توانند از منابع مختلفی ازجمله سامانه عامل‌ها، ماشین‌های مجازی، کانتینرها، پایگاه‌داده‌ها و خدمات ابری جمع‌آوری شوند.

ب) ذخیره‌سازی و مدیریت رویدادها[۲]: بعد از جمع‌آوری رویدادها، این داده‌ها باید در یک سامانه ذخیره‌سازی مناسب ذخیره شوند تا امکان تحلیل و پردازش آن‌ها فراهم باشد. رویدادها معمولاً به‌صورت بی‌درنگ در پایگاه داده‌های سری زمانی یا ابزارهای مدیریت لاگ ذخیره می‌شوند.

ج) تحلیل و پردازش رویدادها[۳]: در این مرحله، داده‌های مربوط به رویدادهای جمع‌آوری‌شده تحلیل می‌شوند تا شاخص‌های

---

[۱] Event Collection
[۲] Event Storage and Management
[۳] Event Processing and Analysis

کلیدی عملکرد (KPIs) از آن‌ها استخراج شوند. تحلیل رویدادها به دو روش اصلی انجام می‌شود:

- تحلیل بی‌درنگ: داده‌های رویدادی به‌صورت هم‌زمان و در لحظه تحلیل می‌شوند تا مشکلات فوری شناسایی و رفع شوند.
- تحلیل پس‌رویدادی[۱]: پس از رخ دادن رویدادها، داده‌ها به‌صورت تاریخی تحلیل می‌شوند تا روندها، نقاط ضعف و بهبودهای لازم شناسایی شوند.

د) شناسایی الگوها و مشکلات عملکردی: از طریق تحلیل رویدادها، می‌توان الگوهایی مانند افزایش تعداد خطاها، رخدادهای امنیتی مشکوک، یا کندی در عملکرد خدمات را شناسایی کرد. این نوع تحلیل به بهبود عملکرد و جلوگیری از خرابی‌های بزرگ‌تر کمک می‌کند.

شاخص‌های کلیدی قابل استخراج از رویدادها:

۱. نرخ رخدادهای موفق و ناموفق: درصد موفقیت درخواست‌ها یا عملیات‌ها که نشان‌دهنده پایداری خدمات است.
۲. تعداد خطاها: تعداد خطاها و مشکلات سامانه که در طی زمان رخ داده است.
۳. میانگین زمان پاسخگویی رویدادها: زمانی که طول می‌کشد تا سامانه به یک رویداد پاسخ دهد.
۴. رخدادهای امنیتی: تعداد و نوع رویدادهای مرتبط با حملات سایبری یا نقض‌های امنیتی.
۵. رخدادهای مقیاس‌پذیری: رویدادهایی که مرتبط با تغییرات در مقیاس منابع سامانه هستند (مثل افزایش یا کاهش تعداد ماشین‌های مجازی).

هـ) بصری‌سازی و گزارش‌گیری رویدادها[۲]: یکی از بخش‌های مهم رصد رویدادهای ابری، نمایش نتایج تحلیل به‌صورت بصری است. ابزارهای بصری‌سازی کمک می‌کنند تا داده‌های مربوط به رویدادها در قالب داشبوردهای تعاملی و گرافیکی نمایش داده شوند.

- **ابزارهای ذخیره‌سازی**
  - Elasticsearch: برای ذخیره و جستجوی سریع رویدادها و لاگ‌های سامانه.
  - Splunk: ابزاری قوی برای ذخیره‌سازی و تحلیل داده‌های رویداد و لاگ‌ها.
  - Fluentd: یک ابزار منبع‌باز برای جمع‌آوری و انتقال لاگ‌ها و رویدادها به سامانه‌های ذخیره‌سازی.
- **انواع رویدادها و شاخص‌های مرتبط**

الف) رویدادهای عملکردی[۳]: این رویدادها مربوط به عملکرد خدمات ابری هستند و شامل اطلاعاتی درباره وضعیت اجرای سرویس‌ها، درخواست‌ها و پاسخ‌ها و تغییرات در وضعیت سامانه می‌باشند. شاخص‌های مرتبط با این رویدادها شامل:

- نرخ درخواست‌ها: تعداد درخواست‌هایی که خدمات در هر لحظه دریافت می‌کند،
- زمان پاسخگویی خدمات: مدت زمانی که خدمات برای پاسخ به درخواست کاربران نیاز دارد.
- نرخ موفقیت عملیات‌ها: درصد عملیات‌هایی که بدون خطا انجام می‌شوند.

ب) رویدادهای امنیتی: رویدادهای امنیتی شامل هر نوع فعالیت مشکوک یا نقض امنیتی است که در خدمات ابری رخ می‌دهد. برخی از شاخص‌های کلیدی امنیتی عبارت‌اند از

- تعداد تلاش‌های ناموفق برای ورود: تعداد تلاش‌هایی که برای ورود به سامانه انجام می‌شود ولی با شکست مواجه می‌شود.

---

[۱] Post-event Analysis
[۲] Visualization and Reporting
[۳] Operational Events

- رخدادهای دسترسی غیرمجاز: هرگونه تلاش برای دسترسی به منابع بدون داشتن مجوزهای لازم.
- حملات DDoS: رویدادهای مرتبط با حملات منع خدمات که می‌تواند عملکرد خدمات را مختل کند.

ج) رویدادهای مرتبط با خرابی[۱]: این نوع رویدادها زمانی رخ می‌دهند که سامانه دچار خرابی یا خطای جدی می‌شود. شاخص‌های مرتبط با این رویدادها شامل:

- زمان خرابی[۲]: مدت زمانی که خدمات به دلیل خرابی یا مشکل غیرقابل دسترسی است.
- تعداد رخدادهای خرابی: تعداد دفعاتی که خدمات دچار قطعی شده است.
- میانگین زمان تعمیر (MTTR[۳]): میانگین زمانی که برای رفع یک مشکل یا خرابی نیاز است.

د) رویدادهای مقیاس‌پذیری[۴]: این نوع رویدادها زمانی رخ می‌دهند که منابع سامانه برای مقابله با تغییرات بار کاری افزایش یا کاهش پیدا می‌کنند. شاخص‌های مرتبط شامل:

- نرخ تغییرات در منابع: تعداد دفعاتی که منابع سامانه مانند ماشین‌های مجازی یا کانتینرها افزایش یا کاهش پیدا کرده‌اند.
- زمان مقیاس‌پذیری[۵]: زمانی که طول می‌کشد تا منابع جدید به سامانه اضافه یا از آن حذف شوند.
- ابزارهای مبتنی‌بر رویداد.
- AWS CloudTrail: خدمات ابری که به رصد و لاگ‌گذاری رویدادهای مختلف در زیرساخت AWS می‌پردازد.
- Azure Event Grid: سرویسی که امکان مدیریت و پاسخگویی به رویدادها در محیط Azure را فراهم می‌کند.

- **مزایای استفاده از روش‌های مبتنی‌بر رویداد**

- پاسخ سریع به رویدادها: این روش امکان شناسایی سریع رویدادهای بحرانی و انجام اقدامات لازم را فراهم می‌کند.
- بهبود امنیت و عملکرد: با پایش دقیق رویدادها، می‌توان به بهبود امنیت و عملکرد کلی زیرساخت ابری کمک کرد.

- **معایب استفاده از روش‌های مبتنی‌بر رویداد**

- پیچیدگی در مدیریت رویدادها: مدیریت و تحلیل حجم بالای رویدادها ممکن است پیچیده و زمان‌بر باشد.
- وابستگی به سرویس‌دهنده: استفاده از ابزارهای مبتنی‌بر رویداد ممکن است سازمان‌ها را به سرویس‌دهنده ابری وابسته کند[۲].

۳-۷- روش‌های مبتنی کانتینر

با گسترش استفاده از کانتینرها و پلتفرم‌های مدیریت و نگهداری[۶] مانند Kubernetes، نیاز به روش‌های خاصی برای رصد و پایش این محیط‌ها احساس می‌شود. این روش‌ها به شناسایی مشکلات کانتینرها و مدیریت عملکرد آن‌ها کمک می‌کنند.

کانتینرها محیط‌های اجرایی سبک و قابل حمل هستند که نرم‌افزارها و وابستگی‌های آن‌ها را به‌صورت یکپارچه و مجزا از سامانه عامل اصلی اجرا می‌کنند. این ویژگی‌ها به توسعه‌دهندگان امکان می‌دهد که اپلیکیشن‌ها را به‌طور مؤثر در محیط‌های مختلف اجرا کنند و به مقیاس‌پذیری سریع و بهبود بهره‌وری کمک کنند.

---

۱ Failure Events
۲ Downtime
۳ Mean Time to Repair
۴ Scalability Events
۵ Scaling Time
۶ Orchestration

برای رصد مؤثر کانتینرها، لازم است که داده‌ها به‌طور دقیق جمع‌آوری، ذخیره‌سازی و تحلیل شوند. مراحل اصلی عبارت‌اند از:

الف) جمع‌آوری داده‌های کانتینر[۱]: جمع‌آوری داده‌های مربوط به کانتینر شامل اطلاعاتی ازجمله مصرف منابع، وضعیت اجرا و وقایع داخلی کانتینر است.

ب) ذخیره‌سازی و مدیریت داده‌های کانتینر[۲]: داده‌های جمع‌آوری‌شده باید در سامانه‌های مناسب ذخیره شوند تا تحلیل و پردازش آن‌ها تسهیل شود. این داده‌ها معمولاً در پایگاه داده‌های سری زمانی یا سامانه‌های ذخیره‌سازی لاگ ذخیره می‌شوند.

ج) تحلیل داده‌های کانتینر[۳]: تحلیل داده‌های جمع‌آوری‌شده شامل بررسی شاخص‌های عملکردی و شناسایی الگوهای مرتبط با مشکلات است. تحلیل داده‌ها به دو روش بلادرنگ و تاریخی انجام می‌شود.

شاخص‌های کلیدی قابل استخراج:

۱. استفاده از منابع[۴]: میزان استفاده از منابع (CPU، حافظه، دیسک) در هر کانتینر.
۲. زمان پاسخگویی[۵]: زمان لازم برای اجرای درخواست‌ها درون کانتینر.
۳. تعداد درخواست‌ها و خطاها[۶]: تعداد درخواست‌های موفق و ناموفق به کانتینر.
۴. پهنای باند شبکه[۷]: نرخ داده‌هایی که توسط کانتینر ارسال و دریافت می‌شود.
۵. سلامت کانتینر[۸]: وضعیت سلامت و فعال بودن کانتینرها.

د) بصری‌سازی و گزارش‌گیری[۹]: پس از تحلیل داده‌ها، نتایج باید به‌صورت بصری نمایش داده شوند تا کاربران بتوانند وضعیت و عملکرد کانتینرها را به‌طور مؤثر مشاهده کنند.

- **ابزارهای ذخیره‌سازی**
  - InfluxDB: پایگاه داده‌ای برای ذخیره‌سازی و مدیریت داده‌های سری زمانی.
  - Elasticsearch: پایگاه داده‌ای برای ذخیره‌سازی و جستجو در داده‌های لاگ و رویدادها.
  - OpenTSDB: پایگاه داده‌ای برای ذخیره‌سازی مقادیر سری زمانی در مقیاس بزرگ.
- **انواع داده‌های مربوط به کانتینر و شاخص‌های کلیدی**

الف) داده‌های عملکردی[۱۰]: این داده‌ها شامل اطلاعاتی درباره عملکرد کانتینرها هستند و می‌توانند به شناسایی مشکلات عملکردی کمک کنند.

- مصرف CPU و حافظه: میزان استفاده از منابع پردازشی و حافظه توسط کانتینر.
- زمان پاسخگویی: مدت زمانی که طول می‌کشد تا یک درخواست درون کانتینر پردازش شود.
- نرخ درخواست‌ها و خطاها: تعداد درخواست‌های موفق و ناموفق پردازش‌شده توسط کانتینر.

---

۱ Container Data Collection
۲ Container Data Storage and Management
۳ Container Data Analysis
۴ Resource Utilization
۵ Response Time
۶ Request and Error Rate
۷ Network Bandwidth
۸ Container Health
۹ Visualization and Reporting
۱۰ Performance Data

ب) داده‌های وضعیت کانتینر[۱]: این داده‌ها اطلاعاتی درباره وضعیت کنونی و سلامت کانتینرها ارائه می‌دهند.

- Uptime: مدت زمانی که کانتینر به‌طور مداوم در حال اجرا است.
- وضعیت سلامت: بررسی وضعیت سلامت و پایداری کانتینر.
- وضعیت خطاها: تعداد و نوع خطاهایی که در کانتینر رخ داده است.

ج) داده‌های شبکه[۲]: این داده‌ها شامل اطلاعاتی درباره تعاملات شبکه‌ای کانتینرها هستند.

- پهنای باند مصرفی: نرخ داده‌ای که توسط کانتینر ارسال و دریافت می‌شود.
- تأخیر شبکه: زمان لازم برای انتقال داده‌ها بین کانتینرها و سایر اجزای سامانه.

د) داده‌های مقیاس‌پذیری[۳]: این داده‌ها اطلاعاتی درباره توانایی کانتینرها برای مقیاس‌پذیری ارائه می‌دهند.

- تعداد کانتینرهای فعال: تعداد کانتینرهایی که به‌طور هم‌زمان در حال اجرا هستند.
- زمان مقیاس‌پذیری: مدت زمانی که طول می‌کشد تا کانتینرها به تعداد مشخصی افزایش یا کاهش یابند.

- **ابزارهای روش‌های استخراج کانتینرها**

- Prometheus[۴]: ابزاری منبع باز برای جمع‌آوری و پایش داده‌های عملکردی از کانتینرها و پادها در محیط Kubernetes.
- Grafana: ابزاری برای بصری‌سازی داده‌های جمع‌آوری شده که به تحلیل و نمایش وضعیت کانتینرها و خدمات مرتبط کمک می‌کند.

- **مزایای استفاده از روش‌های مبتنی‌بر کانتینر**

- دید جامع از کانتینرها: این روش به تیم‌های عملیاتی امکان می‌دهد تا وضعیت کانتینرها و پادها[۵] را به دقت پایش کنند.
- بهبود عملکرد و دسترس‌پذیری: با شناسایی مشکلات عملکردی، می‌توان به بهبود دسترس‌پذیری و کارایی خدمات کمک کرد.

- **معایب استفاده از روش‌های مبتنی‌بر کانتینر**

- پیچیدگی پیاده‌سازی: روش‌های استخراج کانتینرها و پلتفرم‌های همنواسازی نیاز به دانش تخصصی و ابزارهای خاص دارد.
- نیاز به منابع زیاد: مدیریت و پایش حجم بالای کانتینرها و خدمات مرتبط ممکن است منابع پردازشی و ذخیره‌سازی زیادی نیاز داشته باشد[۱۱].

۳-۸- روش‌های مبتنی‌بر هوش مصنوعی/یادگیری ماشین

روش‌های مبتنی‌بر هوش مصنوعی و یادگیری ماشین به طور فزاینده‌ای در رصد و پایش خدمات ابری مورد استفاده قرار می‌گیرند. این روش‌ها به شناسایی الگوهای پیچیده، پیش‌بینی خرابی‌ها و بهینه‌سازی عملکرد خدمات کمک می‌کنند.

---

[۱] Container Status Data
[۲] Network Data
[۳] Scalability Data
[۴] Prometheus
[۵] - پاد (Pod) در Kubernetes، کوچک‌ترین و ابتدایی‌ترین واحد قابل استقرار است. پادها در Kubernetes برای مدیریت و هماهنگی کانتینرها طراحی شده‌اند. یک پاد ممکن است شامل یک یا چند کانتینر باشد که به‌طور مشترک منابع (مانند فضای ذخیره‌سازی و شبکه) را استفاده می‌کنند.

- **ابزارهای مبتنی‌بر هوش مصنوعی**

- Dynatrace: ابزاری پیشرفته که با استفاده از هوش مصنوعی به رصد و پایش خدمات ابری می‌پردازد و به شناسایی خودکار مشکلات کمک می‌کند.
- هوش مصنوعی Datadog[۱]: سرویسی که از الگوریتم‌های یادگیری ماشین برای تحلیل داده‌ها و شناسایی الگوهای غیرعادی در خدمات ابری استفاده می‌کند.

- **مزایایی استفاده از روش‌های مبتنی‌بر هوش مصنوعی /یادگیری ماشین**

- شناسایی الگوهای پیچیده: این روش‌ها به شناسایی الگوهای پیچیده و غیرعادی که به طور معمول قابل شناسایی نیستند، کمک می‌کنند.
- پیش‌بینی خرابی‌ها: با تحلیل داده‌ها و پیش‌بینی خرابی‌های احتمالی، می‌توان از بروز مشکلات بزرگ‌تر جلوگیری کرد.

- **معایب استفاده از روش‌های مبتنی‌بر هوش مصنوعی /یادگیری ماشین**

- پیچیدگی و هزینه: استفاده از ابزارهای مبتنی‌بر هوش مصنوعی نیاز به دانش تخصصی و منابع مالی زیادی دارد.
- وابستگی به الگوریتم‌ها: دقت و کارایی این روش‌ها به کیفیت و دقت الگوریتم‌های یادگیری ماشین بستگی دارد[۱۲].

۳-۹- روش مبتنی‌بر دامنه

در روش مبتنی‌بر دامنه ابتدا دامنه‌های با Country Code Top-Level Domain (.ir) مدنظر را از منابع مختلف جمع‌آوری کرده و یک لیست از دامنه‌های یکتا تهیه می‌شود. در گام بعدی به شناسایی IP و NS[۲] دامنه‌ها می‌پردازیم که الگوریتم‌های مربوط به آن در زیر آورده شده است. در گام بعدی دسته‌بندی IP و NS[۳] براساس Public cloud، private cloud، semi public cloud، انجام می‌شود.

برای بررسی IP و NS دامنه‌ها و حذف دامنه‌هایی که فاقد IP و Name Server معتبر هستند از فرآیندهایی که در زیر توضیح داده شده است، استفاده می‌شود. این فرآیندها به چک کردن وجود و اعتبار IP و NS دامنه‌ها کمک می‌کند تا دامنه‌های فاقد اطلاعات معتبر از لیست رتبه‌بندی حذف شوند. مراحل این فرآیندها به شرح زیر است [۱۳] [۱۴]:

۱. جمع‌آوری داده‌ها از DNS

اولین مرحله، استفاده از خدمات DNS برای استخراج اطلاعات IP و Name Server مربوط به دامنه‌ها است.

- DNS Lookup (پرس‌وجوی DNS): با استفاده از درخواست‌های DNS، می‌توان به‌طور مستقیم آدرس IP مرتبط با یک دامنه و همچنین اطلاعات NameServer را به‌دست آورد.
- IP Address: آدرس IP دامنه‌ای است که به آن متصل می‌شود و نشان‌دهنده‌ی سروری است که وب‌سایت روی آن میزبانی می‌شود.
- Name Server: سرورهای DNS هستند که مسئول پاسخگویی به درخواست‌های DNS برای دامنه‌ی مشخص شده‌اند. Name Server ها اطلاعات مربوط به محل قرارگیری وب‌سایت در اینترنت (IP Address) را ذخیره و مدیریت می‌کنند.

---

[۱] Datadog AI
[۲] Name Server
[۳] Name Server

۲. انجام پرس‌وجوی DNS برای هر دامنه

برای هر دامنه موجود در لیست اولیه، پرس‌وجوی DNS انجام می‌شود تا اطلاعات مربوط به IP و NameServer استخراج شود. این پرس‌وجو معمولاً شامل استفاده از دستوراتی مانند `dig` یا `nslookup` به صورت زیر است:

- دستور dig:

```
dig example.com
```

این دستور اطلاعاتی مانند آدرس‌های IP و Name Server دامنه را نمایش می‌دهد.

- دستور nslookup:

```
nslookup example.com
```

این دستور نیز مشابه dig عمل می‌کند و اطلاعات مربوط به IP و Name Server را بازمی‌گرداند.

۳. بررسی وجود IP Address و Name Server

پس از دریافت نتایج پرس‌وجوی DNS، الگوریتم چک می‌کند که آیا دامنه دارای یک آدرس IP معتبر است یا خیر. همچنین بررسی می‌کند که آیا Name Server های معتبر برای دامنه وجود دارند.

- اگر دامنه‌ای فاقد آدرس IP باشد (یعنی هیچ رکورد A یا AAAA برای دامنه پیدا نشود)، آن دامنه از لیست حذف می‌شود، زیرا نمی‌توان به آن دامنه دسترسی پیدا کرد.
- اگر دامنه‌ای فاقد NameServer باشد (یعنی هیچ رکورد NS برای دامنه پیدا نشود یا NameServer ها به‌درستی تنظیم نشده باشند)، آن دامنه نیز حذف می‌شود، چراکه این نشان‌دهنده مشکل در تنظیمات DNS دامنه است.

۴. بررسی وضعیت IP ها

- علاوه بر وجود IP Address، الگوریتم ممکن است وضعیت و نوع آدرس IP را نیز بررسی کند:
- آدرس IP عمومی یا خصوصی: اگر دامنه دارای یک IP خصوصی باشد (مثل IP های شروع‌شده با ۱۹۲,۱۶۸. یا ۱۰,۰,۰,۰)، این IP معتبر برای اینترنت عمومی نیست و دامنه از لیست حذف می‌شود.
- IP های شناخته‌شده اسپم: برخی IP ها ممکن است در لیست‌های سیاه قرار داشته باشند (به دلیل استفاده برای فعالیت‌های اسپم یا بدافزار). دامنه‌هایی که به این IP ها متصل هستند ممکن است از لیست حذف شوند.

۵. اعتبارسنجی Name Server ها

- پس از دریافت اطلاعات NS، الگوریتم اعتبار NameServer ها را نیز بررسی می‌کند. دامنه‌هایی که NameServer معتبر ندارند یا NameServer هایشان به‌درستی پاسخ نمی‌دهند، از لیست حذف می‌شوند.
- بررسی پاسخ‌دهی NameServer ها: در رتبه بندی ترانکو[۱] چک می‌شود که آیا Name Server ها به درخواست‌های DNS به‌درستی پاسخ می‌دهند یا خیر. اگر Name Server به‌درستی پیکربندی نشده باشد یا خراب باشد، این دامنه فاقد اعتبار خواهد بود و حذف می‌شود.

۶. حذف دامنه‌های فاقد IP یا Name Server معتبر

در پایان، هر دامنه‌ای که:

- آدرس IP نداشته باشد.

---

[۱] Tranco

- Name Server معتبر نداشته باشد.
- یا IP آن معتبر نباشد (خصوصی یا بلاک‌شده باشد)،

به‌طور خودکار از لیست حذف می‌شود.

- **ابزارهای معمول برای بررسی DNS**

۱. dig: یک ابزار خط فرمانی برای اجرای درخواست‌های DNS و دریافت اطلاعات دامنه.

```
dig example.com
```

dig NS example.com بررسی Name Server ها

۲. nslookup: ابزار دیگری برای دریافت اطلاعات DNS مربوط به دامنه.

```
nslookup example.com
```

۳. whois: برای دریافت اطلاعات رجیستری دامنه و اطلاعات DNS نیز مفید است.

این فرآیند، فرآیند بررسی IP و NS دامنه‌ها به‌منظور اطمینان از وجود اطلاعات معتبر DNS برای هر دامنه و حذف دامنه‌هایی است که فاقد اطلاعات صحیح هستند. این کار باعث می‌شود که لیست نهایی شامل وب‌سایت‌هایی با دسترسی و پیکربندی معتبر باشد و از دامنه‌های نامعتبر یا خراب جلوگیری کند.

برای دسته‌بندی IP Owner و Name Server (NS) ها بر اساس ارائه‌دهندگان خدمات ابری عمومی و خصوصی در کشور، می‌توان از روش‌های زیر استفاده کرد. این روش‌ها شامل جمع‌آوری اطلاعات، تحلیل داده‌های IP و NS و دسته‌بندی آن‌ها به‌عنوان ارائه‌دهنده خدمات ابری عمومی یا خصوصی است.

الف) جمع‌آوری اطلاعات IP و Name Server

- ابتدا باید اطلاعات مربوط به IP Address و Name Server دامنه‌ها را از طریق پرس‌وجوی DNS به دست آورد. ابزارهایی مثل `dig` یا `nslookup` برای این کار مفید هستند.

digexample.com:

- این دستور اطلاعات مربوط به آدرس IP و Name Server دامنه را نشان می‌دهد.
- همچنین می‌توان از `whois` برای دریافت اطلاعات رجیستری دامنه و IP مالک (Owner) استفاده کنید.

ب) شناسایی مالک IP Address (IP Owner)

برای شناسایی مالکیت IP و تعیین اینکه یک آدرس IP به کدام ارائه‌دهنده خدمات ابری یا شرکت تعلق دارد، از ابزارهای WHOIS استفاده می‌شود:

- WHOIS یک پایگاه داده عمومی است که اطلاعات مالکیت دامنه و آدرس IP را ارائه می‌دهد و با استفاده از دستور زیر می‌توانید مالک IP را بررسی می‌شود:

```
whois <IP_address>
```

- در اطلاعات خروجی، معمولاً نام مالک IP (ارائه‌دهنده خدمات یا مرکز داده) و موقعیت جغرافیایی آن مشخص می‌شود.

ج) شناسایی Name Server (NS)

Name Server ها معمولاً با نام شرکت‌های ارائه‌دهنده خدمات DNS مرتبط هستند. اطلاعات NS را می‌توان با استفاده از `dig NS` به‌دست آورد:

```
dig NS example.com
```

این دستور سرورهای DNS را که مسئول دامنه هستند، مشخص می‌کند. سپس می‌توان با استفاده از اطلاعات WHOIS، مالک سرورهای DNS را بررسی نمود [۱۳] [۱۴].

- **دسته‌بندی بر اساس ارائه‌دهنده خدمات ابری عمومی یا خصوصی**

برای اینکه مشخص شود یک IP Address یا Name Server به یک ارائه‌دهنده خدمات ابری عمومی یا خصوصی در کشور تعلق دارد، باید اطلاعات زیر بررسی شود:

الف) ارائه‌دهندگان خدمات ابری عمومی

این دسته شامل شرکت‌هایی است که خدمات ابری عمومی ارائه می‌دهند. در کشور، برخی از معروف‌ترین ارائه‌دهندگان خدمات ابری عمومی عبارت‌اند از: ابر آروان، گرین پلاس، پارس‌پک، هاست‌ایران و ابر مبین‌نت.

برای دسته‌بندی IP ها و NS های مرتبط با این شرکت‌ها به صورت زیر اقدام می‌شود:

- پس از دریافت اطلاعات مالکیت IP از WHOIS، بررسی شود که آیا IP یا NS به یکی از این شرکت‌های ارائه‌دهنده خدمات ابری عمومی تعلق دارد یا خیر.
- اگر اطلاعات مربوط به مالکیت IP نشان‌دهنده یکی از این شرکت‌ها بود، آن را به‌عنوان ارائه‌دهنده خدمات ابری عمومی دسته‌بندی شود.

ب) ارائه‌دهندگان خدمات ابری خصوصی

این دسته شامل شرکت‌هایی است که خدمات ابری را برای شرکت‌ها و سازمان‌های خاص به‌صورت خصوصی ارائه می‌دهند. در کشور، بسیاری از شرکت‌های بزرگ یا سازمان‌ها از زیرساخت‌های ابری خصوصی استفاده می‌کنند.

- اگر مالکیت IP Address یا Name Server به یک شرکت یا سازمان خاص (نه یک شرکت عمومی) تعلق داشته باشد، می‌توان فرض کرد که این IP ها به زیرساخت‌های ابری خصوصی مربوط هستند.
- برخی از شرکت‌های خصوصی که زیرساخت ابری دارند، مانند شرکت‌های نفت و گاز یا بانک‌ها، ممکن است دارای IP های مخصوص به خود باشند.

ج) استفاده از پایگاه‌های داده عمومی

- برخی از پایگاه‌های داده عمومی مانند IPinfo، MaxMind یا RIPE NCC می‌توانند کمک کنند تا اطلاعات بیشتری درباره‌ی مالکیت IP ها و دسته‌بندی آن‌ها بر اساس ارائه‌دهنده خدمات ابری به دست آورد.
- این پایگاه‌ها می‌توانند به ما بگویند که یک IP به کدام مرکز داده یا شرکت ارائه‌دهنده خدمات تعلق دارد.

ابرهای عمومی معمولاً توسط شرکت‌های بزرگی ارائه می‌شوند که خدمات متنوعی ازجمله CDN، ذخیره‌سازی و پردازش ابری ارائه می‌دهند. به عنوان مثال:

- IP ها و NS های مرتبط با ابر آروان معمولاً به خدمات عمومی این شرکت متصل هستند.
- اگر اطلاعات مربوط به IP نشان‌دهنده استفاده از CDN یا شبکه توزیع محتوا باشد، به احتمال زیاد به یک ارائه‌دهنده خدمات ابری عمومی تعلق دارد.
- ابرهای خصوصی معمولاً برای سازمان‌ها و شرکت‌های خاصی تنظیم می‌شوند و IP های مربوط به آن‌ها ممکن است به‌صورت محدود و خصوصی قابل‌استفاده باشند.

پس از شناسایی IP Owner و NS ها، می‌توان داده‌ها را دسته‌بندی کرد و با استفاده از ابزارهای تحلیل داده مانند Excel یا Python،

گزارش‌هایی درباره توزیع IP ها بین ارائه‌دهندگان ابری عمومی و خصوصی ایجاد کرد. مثال‌های دسته‌بندی عبارت‌اند:

- اگر یک دامنه به IP هایی در مرکز داده ابر آروان متصل باشد و Name Server آن نیز به‌وسیله این شرکت ارائه شود، می‌توان نتیجه گرفت که این دامنه از خدمات ابری عمومی استفاده می‌کند.
- اگر IP یا NS مربوط به یک بانک یا سازمان دولتی باشد که معمولاً به خدمات ابری خصوصی وابسته است، می‌توان آن را به‌عنوان ابر خصوصی دسته‌بندی کرد.

برای دسته‌بندی IP و NS براساس ارائه‌دهنده خدمات ابری عمومی یا خصوصی در کشور، نیاز به استفاده از ابزارهای DNS، WHOIS و پایگاه‌های داده IP است. با تجزیه‌وتحلیل اطلاعات مالکیت و دسته‌بندی ارائه‌دهندگان خدمات ابری عمومی مانند ابر آروان و پارس‌پک و مقایسه آن‌ها با شرکت‌ها و سازمان‌هایی که از زیرساخت‌های ابری خصوصی استفاده می‌کنند، می‌توانید دسته‌بندی دقیق انجام داد[۱۳] [۱۴].

۴- الگوی پیشنهادی برای رصد بازار ابری کشور

در راستای تحقق هدف عملیاتی «شکل‌گیری حداقل سه فراهم‌کننده خدمات ابری داخلی با قابلیت تأمین نیازهای زیرساختی، ذخیره‌سازی، پردازشی و سکویی برای همه خدمات پایه داخلی و کسب سهم بازار هشتاد درصدی از کل نیاز خدمات ابری کشور» هفت شاخص کلان عبارت‌اند از:

- شاخص (HHI) برای خدمات ابری
- نسبت خدمات ابری تأمین شده داخلی (اعم از ذخیره‌سازی و پردازشی) در حوزه پیام‌رسان و شبکه اجتماعی، به نیاز کشور از کل نیاز بازار
- نسبت خدمات ابری تأمین شده (اعم از ذخیره‌سازی و پردازشی) در حوزه سایر خدمات پایه به نیاز کشور از کل نیاز بازار
- نسبت خدمات ابری به‌کارگیری شده داخلی (اعم از ذخیره‌سازی و پردازشی) در حوزه دولت الکترونیک، به نیاز کشور مزیت‌بخشی به استفاده از خدمات ابری نسبت به زیرساخت‌های اختصاصی
- وجود حداقل سه شرکت ارائه‌کننده خدمات ابری در کشور
- تأمین حداقل ۸۰ درصد نیاز بازار کشور در حوزه خدمات ابری (IaaS، PaaS، SaaS)

منابع استخراج داده با توجه به ۷ شاخص کلان تعیین شده در جدول ۴۱ آمده است.

جدول ۴۱- شاخص‌های کلان و منابع استخراج داده

ردیف	شاخص‌های کلان	منابع داده‌ای
۱	شاخص (HHI) برای خدمات ابری	صورت‌های مالی CSP ها و میزان استفاده از منابع و تعداد کاربران فعال CSP ها
۲	نسبت خدمات ابری تأمین شده داخلی (اعم از ذخیره‌سازی و پردازشی) در حوزه پیام‌رسان و شبکه اجتماعی، به نیاز کشور از کل نیاز بازار	پیام‌رسان‌ها و شبکه‌های اجتماعی داخلی: شامل روبیکا، ایتا، شاد، بله و سروش (ابر پیام‌رسان)
۳	نسبت خدمات ابری تأمین شده (اعم از ذخیره‌سازی و پردازشی) در حوزه سایر خدمات پایه به نیاز کشور از کل نیاز بازار	ارائه‌دهندگان سایر خدمات پایه

ردیف	شاخص‌های کلان	منابع داده‌ای
۴	نسبت خدمات ابری به‌کارگیری شده داخلی (اعم از ذخیره‌سازی و پردازشی) در حوزه دولت الکترونیک، به نیاز کشور	با توجه به سه سناریو تعریف شده برای ابر دولت در نسخه غیر مصوب ۱۰۷ برنامه هفتم توسعه منابع داده این شاخص CSP ها، زیرساخت یکپارچه‌ی ابر دولت یا پلتفرم یکپارچه ابر دولت است.
۵	مزیت‌بخشی به استفاده از خدمات ابری نسبت به زیرساخت‌های اختصاصی	با توجه به اقدامات اجرایی مشخص شده در هر محور منابع داده‌ای ما برای ارزیابی میزان پیشرفت این شاخص مستندات مربوط تنظیم گری و قوانین مصوب در راستای تنظیم گری در حوزه خدمات ابری، CSP ها است.
۶	وجود حداقل سه شرکت ارائه‌کننده خدمات ابری در کشور	CSP ها، (شناسایی شرکت‌های فراهم‌کننده خدمات ابری)
۷	تأمین حداقل ۸۰ درصد نیاز بازار کشور در حوزه خدمات ابری (IaaS,PaaS,SaaS)	CSP ها

در جدول زیر، روش استخراج شاخص های هفتگانه بر اساس روش های مورد بررسی مشخص شده است. با توجه به اینکه روش‌های استخراج تعیین شده در برخی پارامترهای شاخص‌ها با همدیگر متفاوت است، رویکرد ترکیبی مورد استفاده قرارگرفته است.

جدول ۲- روش‌های استخراج شاخص‌های هفت‌گانه

ردیف	شاخص‌های کلان	پارامترهای ورودی	روش‌های استخراج
۱	شاخص (HHI) برای خدمات ابری	۱- حجم مصرف منابع: استفاده از CPU، حافظه، ذخیره‌سازی و پهنای باند. ۲- تعداد کاربران فعال ۳- ترافیک داده: میزان درخواست‌های پردازش شده یا حجم داده انتقال‌یافته. ۴- درآمد حاصل از خدمات: میزان درآمد هر ارائه‌دهنده از بازار خدمات ابری.	• مبتنی‌بر دامنه • مبتنی‌بر عامل
۲	نسبت خدمات ابری تأمین شده داخلی (اعم از ذخیره‌سازی و پردازشی) در حوزه پیام‌رسان و شبکه اجتماعی، به نیاز کشور از کل نیاز بازار	۱- تعداد کاربران فعال پیام‌رسان‌ها ۲- میزان مصرف منابع (IaaS و PaaS)	• مبتنی‌بر ترافیک شبکه • مبتنی‌بر تله‌متری • مبتنی‌بر هوش مصنوعی
۳	نسبت خدمات ابری تأمین شده (اعم از ذخیره‌سازی و پردازشی) در حوزه سایر خدمات پایه به نیاز کشور از کل نیاز بازار	۱- پایش ظرفیت و میزان استفاده از خدمات پایه: اطلاعات مربوط به زیرساخت‌های ابری در خدمات بومی از طریق نظرسنجی‌ها و تحلیل‌های فنی	• مبتنی‌بر ترافیک • مبتنی تله‌متری • مبتنی‌بر هوش مصنوعی
۴	نسبت خدمات ابری به‌کارگیری شده داخلی (اعم از ذخیره‌سازی و پردازشی) در حوزه دولت الکترونیک، به نیاز کشور	۱- بررسی تعداد رک‌های ابری: جمع‌آوری اطلاعات تعداد رک‌های ابری در مراکز داده دولتی با استفاده از سامانه‌های نظارتی به‌طور منظم ۲- جمع‌آوری اطلاعات از سرویس‌دهندگان دولت: اطلاعات مربوط به مصرف منابع ابری از خدمات دولتی	• مبتنی‌بر ترافیک شبکه • مبتنی‌بر تله‌متری • مبتنی‌بر API

ردیف	شاخص‌های کلان	پارامترهای ورودی	روش‌های استخراج
۵	مزیت‌بخشی به استفاده از خدمات ابری نسبت به زیرساخت‌های اختصاصی	۱-تحلیل هزینه فایده: اطلاعات مربوط به هزینه‌های خدمات ابری و زیرساخت‌های اختصاصی و میزان پذیرش در سازمان‌ها ۲- میزان مهاجرت: بررسی تعداد سازمان‌هایی که به سمت خدمات ابری مهاجرت کرده‌اند و مقایسه آن با زیرساخت‌های اختصاصی.	• مبتنی‌بر نظرسنجی و بررسی میدانی
۶	وجود حداقل سه شرکت ارائه‌کننده خدمات ابری در کشور	۱- پایش مداوم بازار: اطلاعات سهم بازار از گزارش‌های مالی و داده‌های عملکردی به‌صورت سالانه یا شش‌ماهه ۲- محاسبه سهم بازار: با استفاده از نرم‌افزارهای تحلیل مالی، سهم هر شرکت محاسبه و تعداد شرکت‌های با سهم حداقل ۱۰ درصد ۳- نظرسنجی و جمع‌آوری داده‌های مالی شرکت‌های فعال در حوزه خدمات ابری	• مبتنی‌بر تله‌متری • مبتنی‌بر API
۷	تأمین حداقل ۸۰ درصد نیاز بازار کشور در حوزه خدمات ابری (IaaS,PaaS,SaaS)	۱- پایش تعداد سرورهای ابری فعال: تعداد سرورهای فعال برای هر یک از خدمات IaaS، PaaS و SaaS جمع‌آوری و با نیازهای بازار مقایسه شود.	• مبتنی‌بر ترافیک شبکه • مبتنی‌بر تله‌متری • مبتنی‌بر API

۵- رصد بازار ابر کشور با روش مبتنی‌بر دامنه

برای رصد بازار خدمات ابری کشور یکی از روش‌های استخراج پیشنهادی، روش مبتنی‌بر دامنه است. در همین بررسی جمع‌آوری دامنه‌های ir. از منابعی چون لیست رتبه‌بندی tranco، دامنه‌های ثبت شده در eNamad.ir، دامنه‌های ثبت شده در ecunion.ir و دامنه‌های ثبت شده در https://eservices.ito.gov.ir/page/iplist یک لیست یکتا تشکیل شده است.

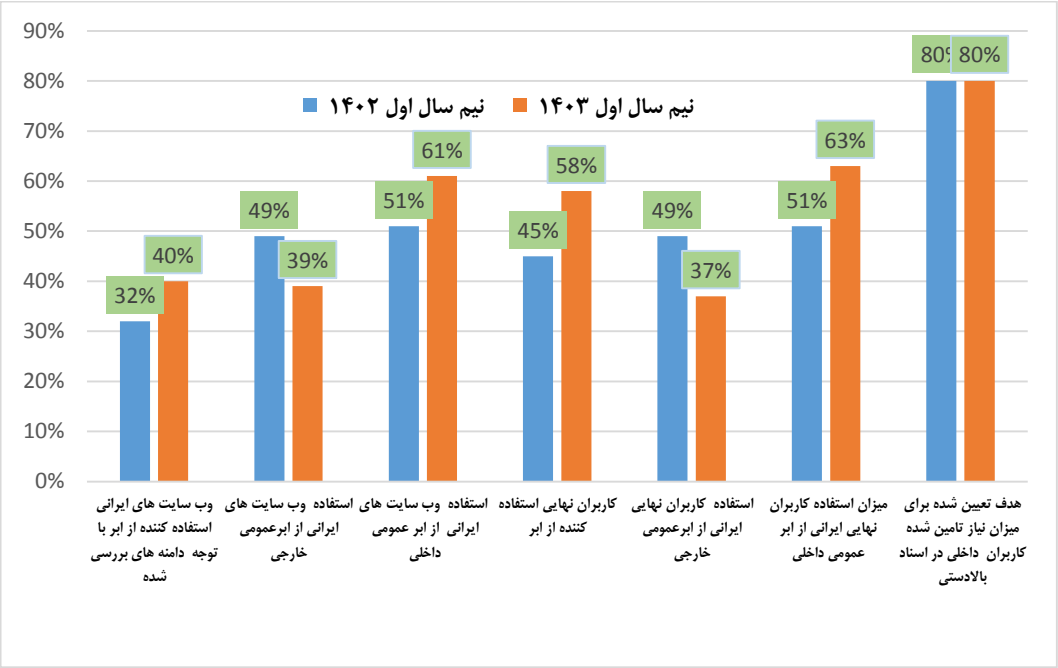
در گام اول، به بررسی IP و NS دامنه‌ها و حذف دامنه‌های فاقد IP و NS (شامل منقضی شدن، اشتباه بودن، فیلتر بودن و...) پرداخته شد.

در گام بعدی به دسته‌بندی دامنه‌ها براساس خدمات گیرنده از خدمات ابری عمومی داخلی و خدمات گیرنده از خدمات ابری خارجی و... پرداخته شده است و سهم شرکت های داخلی و خارجی از بازار خدمات ابری مشخص شده که نتایج آن برای نیم‌سال‌های اول ۱۴۰۲ و نیم‌سال‌های اول ۱۴۰۳ در شکل آورده شده که شامل موارد زیر است:

- در سال ۱۴۰۲ حدود ۱ میلیون و ۵۵۰ هزار دامنه .ir بررسی شد که از این تعداد ۱،۴۷۱،۰۶۷ دامنه فعال بوده‌اند.
- از تعداد ۴۷۰،۷۴۲ وب‌سایت ایرانی از خدمات ابری استفاده می‌کنند که از این تعداد ۲۳۰،۶۶۳ وب‌سایت ایرانی از خدمات ابر عمومی خارجی و ۲۴۰،۰۷۸ وب‌سایت ایرانی از خدمات ابری عمومی داخلی استفاده کرده‌اند.
- در نیم‌سال‌های اول ۱۴۰۳ حدود ۱ میلیون و ۷۰۰ هزار دامنه .ir بررسی شد که از میان آن‌ها ۱،۶۴۹،۸۵۵ دامنه فعال هستند که از تعداد دامنه ۶۵۹،۹۴۲ سایت ایرانی از خدمات ابر عمومی استفاده می‌کنند؛ که از تعداد ۲۵۷،۳۷۸ وب‌سایت ایرانی از خدمات ابر عمومی خارجی و ۴۰۲،۵۶۴ وب‌سایت ایرانی از خدمات ابر عمومی داخلی استفاده می‌کنند.

طبق شکل ، در نیم‌سال‌های اول ۱۴۰۲، ۳۲ درصد و در نیم‌سال‌های اول ۱۴۰۳، ۴۰ درصد وب‌های ایرانی از خدمات ابری استفاده کرده‌اند.

همچنین با توجه به وب‌سایت‌های مشخص شده و کاربران نهایی مشخص شده در نیم‌سال‌های اول ۱۴۰۲، ۴۵ درصد کاربران نهایی ایرانی و در نیم‌سال‌های اول ۱۴۰۳، ۵۶ درصد این کاربران به سمت پذیرش رفته‌اند. از تعداد کاربران در نیم‌سال‌های اول ۱۴۰۲، ۴۹ درصد و نیم‌سال‌های اول ۱۴۰۳، ۳۷ درصد از خدمات ابری خارجی استفاده کرده‌اند. همچنین در سال‌های ۱۴۰۲، ۵۱ درصد و ۱۴۰۳، ۶۳ درصد از خدمات داخلی استفاده کرده‌اند.



شکل ۱- رصد پذیرش و استفاده از خدمات ابری در ایران بر اساس روش مبتنی بر دامنه

۵-۱- تحلیل نتایج

نتایج رصد بازار خدمات ابری کشور نشان می دهد که، با توجه به تسریع در شناسایی نقش‌های اصلی در زیست‌بوم خدمات ابری کشور و اعطای شناسنامه به آن‌ها، شرکت‌ها در یک رقابت مفید در مسیر ارتقای کیفیت خدمات خود و جلب اعتماد کاربران قرار گرفته‌اند. این امر منجر به جلب کاربران داخلی و افزایش پذیرش خدمات ابری داخلی در کشور شده است. از طرفی مصوبات موجود مبنی بر الزام دستگاه‌های اجرایی و شرکت‌ها و سازمان‌ها به استفاده از خدمات ابری شرکت‌های داخلی دارای شناسنامه منجر به رشد در سوق دادن کاربران داخلی به خدمات داخلی شده است. همچنین باعث افزایش سهم شرکت‌های فراهم کننده خدمات ابری عمومی کشور در تأمین نیاز به خدمات ابری کاربران و وب‌سایت‌های داخلی در ابتدای ۱۴۰۳ نسبت ابتدای سال ۱۴۰۲ شده است.

با توجه به فاصله بین نیاز تأمین شده کاربران داخلی در ابتدای سال ۱۴۰۳ در کشور با هدف ۸۰ درصدی مشخص شده در اسناد بالادستی، لازم است برنامه ریزی هماهنگی میان بازیگران در بخش های مختلف برای افزایش عرضه و تقاضا ذیل یک نقشه راه و برنامه ملی انجام گیرد:

- ایجاد زیرساخت‌های ملی برای خدمات ابری
- تشویق سرمایه‌گذاری در خدمات ابری داخلی
- تدوین استانداردهای ملی و بین‌المللی برای خدمات ابری
- حمایت از حقوق و منافع شرکت‌های فعال در حوزه خدمات ابری
- تأمین انرژی پایدار برای مراکز داده
- حمایت مالی از استارت‌اپ‌های خدمات ابری داخلی
- حمایت از تولیدکنندگان سخت‌افزارهای مورد نیاز برای خدمات ابری

در همین زمینه اقدامات پیشنهادی برای برخی از سازمان ها، در جداول زیر اراده شده است.

جدول ۳- برنامه اقدام برای افزایش سهم شرکت‌های فراهم‌کننده خدمات ابری داخلی [۱۵]

متولیان	اقدامات
سازمان فناوری اطلاعات ایران (ICT)	- ارائه بسته‌های تشویقی برای توسعه زیرساخت ابری - تدوین پروتکل‌های امنیت داده برای خدمات ابری داخلی - ایجاد بسترهای ساده برای مهاجرت به خدمات ابری داخلی - ایجاد سامانه مقایسه خدمات ابری
شرکت ارتباطات زیرساخت	- توسعه پهنای باند اختصاصی برای خدمات ابری داخلی - کاهش تعرفه‌های انتقال داده در شبکه ملی اطلاعات - بهینه‌سازی مراکز داده موجود - ارائه دسترسی به زیرساخت‌های اشتراکی و آزاد دولتی برای فراهم‌کنندگان جدید
مرکز مدیریت راهبردی افتا (امنیت فضای تبادل اطلاعات)	- ایجاد استانداردهای ملی امنیت ابری - اجرای برنامه‌های ارزیابی امنیتی مداوم - ایجاد یک مرکز پاسخگویی فوری به رخدادهای امنیتی (CERT) خاص خدمات ابری
پژوهشگاه ارتباطات و فناوری اطلاعات	- تحقیق و توسعه فناوری‌های نوین ابری - ارزیابی و رتبه‌بندی شرکت‌های فراهم‌کننده خدمات ابری داخلی
مرکز ماهر (مدیریت امداد و هماهنگی رخدادهای رایانه‌ای)	- راه‌اندازی سامانه هشدار سریع برای حملات سایبری در حوزه ابری - برگزاری کارگاه‌های امنیت سایبری - تدوین و اجرای سیاست‌های پشتیبانی و بازیابی اطلاعات
سازمان تنظیم مقررات و ارتباطات رادیویی (رگولاتوری)	- ایجاد تعرفه‌های حمایتی برای خدمات ابری داخلی - تدوین استانداردهای فنی برای خدمات ابری

۶- مراجع

[۱] Dabade, T.D. Information technology infrastructure library (ITIL). in Proceedings of the ۴th National Conference. ۲۰۱۲.

[۲] Kaur, P.D. and I. Chana, A resource elasticity framework for QoS-aware execution of cloud applications. Future Generation Computer Systems, ۲۰۱۴. ۳۷: p. ۱۴-۲۵.

[۳] Zhang, Q., L. Cheng, and R. Boutaba, Cloud computing: state-of-the-art and research challenges. Journal of internet services and applications, ۲۰۱۰. ۱: p. ۷-۱۸.

[۴] Velte, A.T., T.J. Velte, and R.C. Elsenpeter, Cloud computing: a practical approach. ۲۰۱۰: McGraw-Hill.

[۵] Buyya, R., J. Broberg, and A.M. Goscinski, Cloud computing: Principles and paradigms. ۲۰۱۰: John Wiley & Sons.

[۶] Vervaet, A., Automated Log-Based Anomaly Detection within Cloud Computing Infrastrucrtures ,۲۰۲۳ . Sorbonne Université.

[۷] Modi, K.J., D.P. Chowdhury, and S. Garg. An Ontology-Based Approach for Automatic Cloud Service Monitoring and Management. in Advances in Big Data and Cloud Computing. ۲۰۱۸. Springer.

[۸] Fatema, K., et al., A survey of cloudmonitoring tools: Taxonomy, capabilities and objectives. Journal of Parallel and Distributed Computing, ۲۰۱۴. ۷۴(۱۰): p. ۲۹۱۸-۲۹۳۳.

[۹] Zhang, L., Wu, Q., Chen, M., Zhang, X., Zhang, Z., & Zhao, F. (۲۰۱۷). A Survey on Cloud Monitoring: Challenges, Methodsand Tools. IEEE Access, ۵, ۱۴۹۲-۱۵۰۹.

[۱۰]Meng, X., V. Pappas, and L. Zhang. Improving the scalability of data center networks with traffic-aware virtual machine placement. in ۲۰۱۰ Proceedings IEEE INFOCOM. ۲۰۱۰. IEEE.

[۱۱]Arunarani, A., D. Manjula, and V .Sugumaran, Task scheduling techniques in cloud computing: A literature survey. Future Generation Computer Systems, ۲۰۱۹. ۹۱: p. ۴۰۷-۴۱۵.

[۱۲]Ghosh, R., Longo, F., Xia, Y., & Padberg, J. (۲۰۱۵). An ontology-based approach for the management of cloud resources. Future Generation Computer Systems, ۴۸, ۱۰-۲۲.

[۱۳]Chandramouli, R. and S. Rose, Secure domain name system (DNS) deployment guide. NIST Special Publication, ۲۰۰۶. ۸۰۰: p. ۸۱-۲.

[۱۴]ندا قربانی، علی شریفی، احسان آریانیان، گزارش "تعیین نحوه استخراج شاخص‌های مورد نیاز رصد خدمات ابری از ارائه‌دهنده خدمات ابری در کشور از بستر شبکه به منظور ارائه در مرکز رصد"، ۱۴۰۳/۰۶/۲۶

[۱۵]ندا قربانی، علی شریفی، پژمان گودرزی، علیرضا منصوری، گزارش " تهیه و تدوین نقشه راه توسعه خدمات ابری کشور و راهکارهای تحقق آن در حوزه خدمات ابری منطبق بر سند توسعه رایانش ابری"، ۱۴۰۳/۰۲/۳۱.

نشانی: تهران، انتهای کارگر شمالی، پژوهشگاه ارتباطات و فناوری اطلاعات، معاونت پژوهش و توسعه ارتباطات علمی

تلفن: ۰۲۱-۸۸۶۳۰۳۵۵

نمابر: ۰۲۱-۸۸۶۳۰۳۵۶