

AIops برای پیش‌بینی و مدیریت خطاهای زیرساخت IT

مقدمه

زیرساخت‌های فناوری اطلاعات در سال‌های اخیر به شدت پیچیده شده‌اند. سازمان‌ها دیگر تنها با چند سرور فیزیکی، تجهیزات شبکه و پایگاه داده‌های محدود سروکار ندارند؛ بلکه معماری‌های ابری، میکروسرویس‌ها، کانتینرها، Kubernetes، محیط‌های چندابری، APIها، سامانه‌های توزیع‌شده و زیرساخت‌های نرم‌افزارمحور، بخش مهمی از محیط‌های مدرن IT را تشکیل می‌دهند. این تحول اگرچه مقیاس‌پذیری، انعطاف‌پذیری و سرعت توسعه را افزایش داده است، اما مدیریت خطا و حفظ قابلیت اطمینان زیرساخت را نیز دشوارتر کرده است.

در چنین محیطی، حجم داده‌های عملیاتی تولیدشده توسط زیرساخت بسیار زیاد است. سرورها، برنامه‌ها، تجهیزات شبکه، پایگاه‌های داده و سرویس‌های ابری به‌طور مداوم Logs، Events و Traces تولید می‌کنند. بررسی دستی این حجم از اطلاعات برای تیم‌های IT تقریباً غیرممکن است. از سوی دیگر، سیستم‌های سنتی مانیتورینگ که عمدتاً بر آستانه‌های ثابت و قواعد از پیش تعریف‌شده تکیه دارند، در بسیاری از محیط‌های پیچیده قادر نیستند روابط میان رویدادهای مختلف را به‌درستی تشخیص دهند.

در این شرایط، AIops یا «هوش مصنوعی برای عملیات فناوری اطلاعات» به‌عنوان رویکردی برای استفاده از هوش مصنوعی و یادگیری ماشین در مدیریت زیرساخت مطرح شده است. هدف AIops تنها شناسایی یک خطا پس از وقوع نیست؛ بلکه تلاش می‌کند با تحلیل داده‌های تاریخی و لحظه‌ای، ناهنجاری‌ها را شناسایی کند، احتمال وقوع Failure را پیش‌بینی کند، رخدادهای مرتبط را به یکدیگر متصل کند، علت ریشه‌ای مشکل را مشخص کند و در برخی شرایط، اقدام اصلاحی مناسب را به‌صورت خودکار انجام دهد.

بنابراین، استدلال اصلی این مقاله آن است که AIops می‌تواند مدیریت زیرساخت IT را از یک مدل واکنشی به سمت مدلی پیش‌نگر و تا حدی خودکار هدایت کند؛ اما میزان موفقیت آن به عواملی مانند کیفیت داده، معماری سیستم، انتخاب مدل، تفسیرپذیری، کنترل Automation و توانایی سازگاری با تغییرات زیرساخت وابسته است.

AIops چیست؟

AIops مخفف Artificial Intelligence for IT Operations است و به استفاده از تکنیک‌های هوش مصنوعی، یادگیری ماشین، تحلیل داده و اتوماسیون برای بهبود عملیات فناوری اطلاعات اشاره دارد.

در یک محیط سنتی، ممکن است برای هر شاخص یک Threshold تعیین شود. برای مثال، اگر مصرف CPU از ۹۰ درصد بیشتر شد، سیستم یک هشدار ایجاد کند. چنین روشی در محیط‌های ساده قابل استفاده است، اما همیشه رفتار واقعی سیستم را منعکس نمی‌کند.

فرض کنید مصرف CPU یک سرویس معمولاً بین ۲۰ تا ۳۰ درصد است و ناگهان به ۶۵ درصد می‌رسد. ممکن است این مقدار از Threshold تعریف‌شده عبور نکرده باشد، اما افزایش ناگهانی آن می‌تواند نشانه یک مشکل باشد. در مقابل، ممکن است

CPU یک سرویس در یک زمان خاص به ۹۵ درصد برسد، ولی این افزایش کاملاً طبیعی باشد، زیرا سرویس در حال پردازش یک Workload برنامه‌ریزی شده است.

AIops تلاش می‌کند به جای بررسی مستقل هر شاخص، الگوی کلی رفتار سیستم را تحلیل کند. به همین دلیل، تفاوت اصلی میان Monitoring سنتی و AIops را می‌توان در حرکت از «نظارت مبتنی بر قواعد» به سمت «تحلیل هوشمند رفتار سیستم» مشاهده کرد.

چرا پیش‌بینی خطا اهمیت دارد؟

در مدیریت زیرساخت IT، هرچه یک Failure زودتر شناسایی شود، فرصت بیشتری برای جلوگیری از پیامدهای آن وجود خواهد داشت.

فرض کنید یک دیسک سرور به تدریج نشانه‌های خرابی نشان می‌دهد. در یک سیستم کاملاً واکنشی، احتمالاً زمانی هشدار جدی ایجاد می‌شود که دیسک از کار افتاده باشد. در یک سیستم پیش‌نگر، داده‌های مربوط به خطاهای سخت‌افزاری، افزایش I/O Errors و سایر نشانه‌ها می‌توانند برای تخمین احتمال Failure مورد استفاده قرار گیرند.

این تفاوت را می‌توان به سه سطح تقسیم کرد:

در عملیات Reactive، ابتدا Failure رخ می‌دهد و سپس تیم IT برای رفع آن اقدام می‌کند.

در عملیات Proactive، نشانه‌های اولیه مشکل شناسایی می‌شوند و تیم پیش از Failure مداخله می‌کند.

در عملیات Predictive، سیستم با استفاده از داده‌های تاریخی و جاری احتمال وقوع Failure در آینده را تخمین می‌زند.

AIops در شکل بالغ خود تلاش می‌کند سازمان را از سطح اول به سطوح دوم و سوم منتقل کند.

منابع داده در AIops

یکی از مهم‌ترین ویژگی‌های AIops، توانایی ترکیب داده‌هایی است که از منابع مختلف تولید می‌شوند.

Metrics

Metrics داده‌های عددی هستند که وضعیت سیستم را در طول زمان نشان می‌دهند: CPU Usage, Memory, Disk Usage, Network Throughput, Latency, Request Rate و Error Rate نمونه‌هایی از این داده‌ها هستند.

این اطلاعات معمولاً به شکل Time Series ذخیره می‌شوند و برای تشخیص ناهنجاری و پیش‌بینی روند آینده اهمیت زیادی دارند.

Logs

Logs اطلاعات متنی یا ساختاریافته‌ای درباره رویدادهای رخ داده در سیستم ارائه می‌کنند.

برای مثال، یک Metric ممکن است فقط نشان دهد که نرخ خطا افزایش یافته است، اما Log می‌تواند دلیل احتمالی آن را به شکل Connection Timeout، Authentication Failure یا Database Error نشان دهد.

Distributed Traces

در معماری‌های Microservices، یک درخواست ممکن است از چندین سرویس عبور کند Distributed Tracing. مسیر این درخواست را ثبت می‌کند و مشخص می‌سازد که در کدام قسمت زنجیره بیشترین تأخیر یا خطا ایجاد شده است.

این اطلاعات برای تحلیل Root Cause بسیار ارزشمند هستند.

Events

رویدادهایی مانند Deployment، Restart شدن Container، تغییر Configuration، Failover و Scaling نیز می‌توانند برای تحلیل Incident استفاده شوند.

داده‌های ITSM

اطلاعات مربوط به Incidentها، Changeها، Problemها و تیکت‌های قبلی نیز می‌توانند به مدل‌های AIops کمک کنند تا الگوهای موجود در رخدادهای گذشته را یاد بگیرند.

ترکیب این منابع داده، یکی از تفاوت‌های اصلی AIops با ابزارهای سنتی مانیتورینگ محسوب می‌شود.

تشخیص ناهنجاری با AIops

Anomaly Detection یا تشخیص ناهنجاری یکی از مهم‌ترین کاربردهای هوش مصنوعی در AIops است.

هدف این فرآیند، شناسایی رفتارهایی است که با الگوی عادی سیستم تفاوت دارند.

روش‌های ساده آماری می‌توانند از میانگین متحرک، انحراف معیار و روش‌های Forecasting برای تعیین محدوده طبیعی رفتار استفاده کنند.

در مدل‌های پیچیده‌تر، الگوریتم‌هایی مانند Isolation Forest، One-Class SVM و Clustering مورد استفاده قرار می‌گیرند.

همچنین مدل‌های Deep Learning مانند Autoencoder، LSTM و Transformerهای زمانی می‌توانند برای تحلیل الگوهای پیچیده Time Series استفاده شوند.

برای مثال، فرض کنید یک سرویس در حالت عادی دارای Latency حدود ۱۰۰ میلی‌ثانیه است. اگر Latency به تدریج به ۱۵۰، ۲۰۰ و سپس ۳۰۰ میلی‌ثانیه برسد، یک مدل هوشمند می‌تواند این روند را پیش از آنکه سرویس کاملاً دچار مشکل شود شناسایی کند.

پژوهش‌های انجام‌شده در حوزه AIOps نشان می‌دهند که تشخیص ناهنجاری در داده‌های سری زمانی یکی از موضوعات مهم در مدیریت Failure و تحلیل KPI های سیستم‌های IT است.

تفاوت Failure Prediction و Anomaly Detection

این دو مفهوم به یکدیگر مرتبط هستند، اما یکسان نیستند.

Anomaly Detection به این پرسش پاسخ می‌دهد:

«آیا رفتار فعلی سیستم غیرعادی است؟»

Failure Prediction سؤال متفاوتی مطرح می‌کند:

«با توجه به رفتار فعلی و تاریخی سیستم، احتمال وقوع Failure در آینده چقدر است؟»

از دیدگاه یادگیری ماشین، Failure Prediction می‌تواند به صورت یک مسئله Classification تعریف شود. در این حالت، مدل ممکن است برای یک بازه زمانی مشخص احتمال Failure را تخمین بزند.

برای مثال:

احتمال Failure در ۳۰ دقیقه آینده: ۸۲ درصد

البته این عدد به تنهایی کافی نیست. یک سیستم حرفه‌ای باید مشخص کند که چه عواملی در ایجاد این پیش‌بینی نقش داشته‌اند.

برای مثال، مدل ممکن است افزایش Memory Usage، کاهش Throughput و افزایش Error Rate را مهم‌ترین عوامل تشخیص داده باشد.

نقش Time-Series Forecasting

بخش قابل توجهی از مشکلات زیرساختی با روندهای زمانی قابل تشخیص هستند.

برای مثال، اگر مصرف Storage یک سازمان به شکل پیوسته افزایش پیدا کند، مدل Forecasting می‌تواند تخمین بزند که چه زمانی ظرفیت موجود به محدوده بحرانی خواهد رسید.

این موضوع در مدیریت:

- Storage
- CPU
- Memory
- Network Capacity
- Cloud Resources

• Database Capacity

کاربرد دارد.

در یک سیستم پیشرفته، پیش‌بینی تنها به نمایش یک نمودار محدود نمی‌شود. سیستم باید بتواند بر اساس پیش‌بینی، پیشنهاد عملیاتی ارائه کند.

برای مثال:

«با توجه به روند مصرف فعلی، ظرفیت Storage در ۱۸ روز آینده به محدوده بحرانی خواهد رسید».

چنین اطلاعاتی به تیم IT فرصت می‌دهد پیش از وقوع مشکل، ظرفیت را افزایش دهد.

Alert Fatigue و Event Correlation کاهش

یکی از مشکلات رایج در مراکز عملیات IT، تعداد بسیار زیاد هشدارها است.

فرض کنید یک Database دچار مشکل شده باشد. این Failure ممکن است باعث ایجاد ده‌ها یا صدها Alert شود:

افزایش Database Latency، خطای Connection، افزایش API Error، افزایش Request Timeout و کاهش Throughput.

اگر تمام این موارد به صورت مستقل نمایش داده شوند، اپراتور ممکن است تصور کند با چندین مشکل مختلف مواجه است.

AIops می‌تواند بر اساس زمان وقوع، وابستگی سرویس‌ها، توپولوژی زیرساخت و الگوهای تاریخی، این رخدادها را به یک Incident مشترک مرتبط کند.

در نتیجه به جای مشاهده صدها هشدار، تیم ممکن است با یک Incident اصلی مواجه شود:

«اختلال در اتصال سرویس Application به Database»

این قابلیت می‌تواند حجم Noise را کاهش داده و تمرکز تیم عملیات را بر رخدادهای مهم‌تر افزایش دهد.

Root Cause Analysis

یکی از دشوارترین وظایف در مدیریت زیرساخت، پیدا کردن علت ریشه‌ای مشکل است.

برای مثال، ممکن است کاربران کاهش سرعت یک Application را گزارش کنند. بررسی اولیه نشان می‌دهد API ها کند شده‌اند. بررسی عمیق‌تر نشان می‌دهد Backend Service با Timeout مواجه است و در نهایت مشخص می‌شود که Database Latency افزایش یافته است.

بنابراین:

User Problem → API Latency → Backend Timeout → Database Latency

در این زنجیره، API Timeout لزوماً علت ریشه‌ای نیست؛ بلکه ممکن است پیامد یک مشکل در Database باشد.

AIOps با ترکیب Logs، Metrics، Traces و Topology می‌تواند این روابط را تحلیل کند.

این مسئله در معماری‌های Microservices اهمیت بسیار زیادی دارد، زیرا تعداد زیادی سرویس به یکدیگر وابسته هستند.

کاربرد Graph Neural Networks در AIOps

یکی از رویکردهای پیشرفته برای تحلیل زیرساخت IT، نمایش آن به شکل Graph است.

در این مدل، هر جزء زیرساخت می‌تواند یک Node باشد و وابستگی میان اجزا به شکل Edge نمایش داده شود.

برای مثال:

Database → Backend → API Gateway → Frontend

اگر Database دچار Failure شود، احتمال دارد چندین سرویس دیگر نیز تحت تأثیر قرار گیرند.

Graph Neural Networks یا GNN ها برای چنین ساختاری مناسب هستند، زیرا اطلاعات را میان Node های مرتبط منتقل می‌کنند و می‌توانند روابط ساختاری میان اجزای سیستم را یاد بگیرند.

این روش می‌تواند در Root Cause Analysis، Failure Propagation و Dependency Analysis مورد استفاده قرار گیرد.

Transformer و مدل‌های زبانی در AIOps

Transformer ها ابتدا در حوزه پردازش زبان طبیعی مورد توجه قرار گرفتند، اما قابلیت آن‌ها در پردازش توالی‌های طولانی و وابستگی‌های پیچیده باعث شده است در حوزه‌های دیگری مانند AIOps نیز مورد استفاده قرار گیرند.

در AIOps، Transformer می‌تواند برای تحلیل توالی Alert ها، Logs، Time Series و گزارش‌های Incident استفاده شود.

مدل‌های زبانی بزرگ یا LLM ها نیز امکان تحلیل اطلاعات عملیاتی به زبان طبیعی را فراهم کرده‌اند.

برای مثال، به جای اینکه اپراتور مجبور باشد صدها خط Log را بررسی کند، یک مدل می‌تواند داده‌ها را خلاصه کرده و نتیجه‌ای مانند زیر ارائه دهد:

«افزایش Error Rate سرویس پرداخت از ساعت ۱۵:۱۰ آغاز شده است. این تغییر با Deployment نسخه جدید هم‌زمان بوده و Trace ها افزایش Latency در Database را نشان می‌دهند. دو Incident مشابه در سوابق قبلی پس از Deployment مشابه ثبت شده است.»

چنین قابلیت می‌تواند زمان تحلیل اولیه Incident را کاهش دهد.

با این حال، استفاده از LLM ها بدون کنترل می‌تواند مشکلاتی مانند Hallucination یا ارائه تحلیل نادرست ایجاد کند. بنابراین خروجی مدل باید در عملیات حساس با داده‌های واقعی سیستم و کنترل انسانی اعتبارسنجی شود.

پیش‌بینی Failure در Cloud و Kubernetes

محیط‌های Cloud Native یکی از مهم‌ترین حوزه‌های کاربرد AIops هستند.

در Kubernetes ممکن است در یک لحظه صدها یا هزاران Pod و Container در حال اجرا باشند. این اجزا به‌صورت پویا ایجاد، حذف و جابه‌جا می‌شوند.

در چنین محیطی، استفاده از Threshold های ثابت دشوارتر است.

برای مثال، افزایش CPU یک Pod ممکن است نشانه مشکل باشد یا صرفاً نتیجه افزایش طبیعی Traffic باشد.

بنابراین AIops باید Context را نیز در نظر بگیرد.

این Context می‌تواند شامل Deployment های اخیر، تغییرات Configuration، وضعیت Node ها، Traffic Pattern، Auto-scaling و وابستگی سرویس‌ها باشد.

ترکیب این اطلاعات امکان تصمیم‌گیری دقیق‌تر را فراهم می‌کند.

Predictive Maintenance در زیرساخت IT

AIops تنها برای سرویس‌های نرم‌افزاری کاربرد ندارد و می‌تواند در نگهداری پیش‌بینانه تجهیزات فیزیکی نیز استفاده شود.

در سرورها و تجهیزات شبکه می‌توان اطلاعاتی مانند Temperature، Hardware Error، Disk Error، Memory Error و وضعیت Power Supply را تحلیل کرد.

اگر مدل بتواند الگوهایی را شناسایی کند که معمولاً قبل از خرابی سخت‌افزار ظاهر می‌شوند، سازمان می‌تواند قبل از وقوع Failure برای تعمیر یا جایگزینی تجهیز برنامه‌ریزی کند.

در نتیجه، تعمیرات اضطراری می‌تواند به سمت Maintenance برنامه‌ریزی شده حرکت کند.

Automated Remediation و زیرساخت خودترمیم‌شونده

یکی از اهداف پیشرفته AIops، عبور از مرحله تشخیص و ورود به مرحله اقدام خودکار است.

فرض کنید سیستم تشخیص دهد که یک Container دچار وضعیت غیرعادی شده است. در صورتی که سیاست‌های سازمان اجازه دهند، AIops می‌تواند Runbook مربوط به Restart کردن Container را اجرا کند.

اقدامات دیگری مانند Scale Out، Failover، Rollback یا تغییر ظرفیت نیز در برخی محیط‌ها قابل خودکارسازی هستند.

با این حال، Automation باید بر اساس سطح ریسک طراحی شود.

برای عملیات کم‌خطر می‌توان Fully Automated Remediation را در نظر گرفت، اما برای اقداماتی مانند تغییر گسترده Configuration یا Rollback سیستم‌های حیاتی، بهتر است تأیید انسانی در فرآیند باقی بماند.

یک مدل عملیاتی مناسب می‌تواند به شکل زیر باشد:

Recommendation → Human Approval → Automated Execution

این رویکرد میان سرعت و کنترل تعادل ایجاد می‌کند.

ITSM و AIOps

ادغام AIOps با سیستم‌های ITSM می‌تواند چرخه مدیریت Incident را تا حد زیادی خودکار کند.

پس از شناسایی یک مشکل، سیستم می‌تواند:

۱. Incident را شناسایی کند.

۲. رخداد‌های مشابه گذشته را پیدا کند.

۳. علت احتمالی را مشخص کند.

۴. تیم مسئول را تعیین کند.

۵. Priority مناسب را پیشنهاد دهد.

۶. Runbook مرتبط را شناسایی کند.

۷. در صورت مجاز بودن، اقدام اصلاحی را اجرا کند.

۸. نتیجه عملیات را در Ticket ثبت کند.

این فرآیند می‌تواند زمان صرف‌شده برای Triage و بررسی دستی Incident ها را کاهش دهد.

معیارهای ارزیابی AIOps

موفقیت یک پروژه AIOps نباید فقط بر اساس Accuracy مدل سنجیده شود.

معیارهای مهم عبارت‌اند از:

MTTD یا Mean Time to Detect که زمان متوسط شناسایی رخداد را نشان می‌دهد.

MTTR یا Mean Time to Repair/Resolve که مدت زمان لازم برای رفع یا حل Incident را اندازه‌گیری می‌کند.

False Positive Rate که نشان‌دهنده نسبت هشدارهای نادرست است.

False Negative Rate که مشخص می‌کند چه تعداد Failure از دید سیستم پنهان مانده‌اند.

Alert Reduction که میزان کاهش هشدارهای غیرضروری را نشان می‌دهد.

Prediction Lead Time نیز اهمیت زیادی دارد؛ زیرا مشخص می‌کند سیستم چه مدت پیش از وقوع Failure هشدار می‌دهد.

برای مثال، اگر مدل Failure را تنها چند ثانیه پیش از وقوع تشخیص دهد، از نظر علمی ممکن است عملکرد مناسبی داشته باشد، اما ارزش عملیاتی آن محدود است.

چالش کیفیت داده

کیفیت داده یکی از مهم‌ترین عوامل موفقیت AIOps است.

اگر Timestamp های Logs و Metrics هماهنگ نباشند، داده‌ها ناقص باشند یا Incident های قبلی به‌درستی ثبت نشده باشند، مدل نمی‌تواند روابط قابل اعتمادی یاد بگیرد.

یکی دیگر از مشکلات مهم، Class Imbalance است.

Failure ها معمولاً در مقایسه با رخدادهای عادی بسیار کم هستند. ممکن است در میان یک میلیون رکورد تنها چند صد رکورد مربوط به Failure باشد.

در چنین شرایطی Accuracy به‌تنهایی معیار مناسبی نیست. معیارهایی مانند Precision، Recall، F1-Score و PR-AUC می‌توانند تصویر بهتری از عملکرد مدل ارائه دهند.

Concept Drift

زیرساخت‌های IT دائماً تغییر می‌کنند. نسخه نرم‌افزار، معماری، حجم Traffic، Configuration و سرویس‌های مورد استفاده ممکن است در طول زمان تغییر کنند.

در نتیجه، الگوی داده‌ای که مدل در زمان آموزش مشاهده کرده است ممکن است با وضعیت فعلی تفاوت داشته باشد.

این پدیده Concept Drift نامیده می‌شود.

بنابراین، مدل AIOps باید به‌طور مداوم ارزیابی شود و در صورت تغییر رفتار سیستم، احتمالاً نیاز به بازآموزی یا تنظیم مجدد داشته باشد.

به عبارت دیگر، تنها زیرساخت نیست که باید Monitoring شود؛ خود مدل AIops نیز باید تحت Model Monitoring قرار گیرد.

تفسیر پذیری و اعتماد به AIops

اگر یک سیستم اعلام کند که «احتمال Failure برابر ۸۵ درصد است»، تیم عملیات معمولاً می‌خواهد بداند چرا چنین نتیجه‌ای به دست آمده است.

یک سیستم قابل اعتماد باید تا حد امکان عوامل مؤثر در تصمیم خود را نمایش دهد.

برای مثال:

افزایش ۴۵ درصدی Latency

افزایش Error Rate

تغییر Configuration

افزایش Memory Usage

و شباهت با Incident های قبلی

می‌توانند به عنوان شواهد مؤثر در پیش‌بینی نمایش داده شوند.

تفسیر پذیری به اپراتور اجازه می‌دهد تصمیم مدل را ارزیابی کند و در صورت لزوم آن را رد یا اصلاح کند.

امنیت AIops

AIops خود نیز بخشی از زیرساخت حساس سازمان محسوب می‌شود.

اگر سیستم AIops مجوز اجرای عملیات خودکار داشته باشد، دسترسی غیرمجاز به آن می‌تواند خطرناک باشد.

به همین دلیل، استفاده از Least Privilege، کنترل دسترسی مبتنی بر نقش، Audit Logging، Approval Workflow و ثبت دقیق اقدامات ضروری است.

همچنین داده‌های Logs و تیکت‌های ITSM ممکن است شامل اطلاعات حساس باشند. بنابراین Data Governance و کنترل دسترسی به داده‌ها باید از ابتدا در معماری AIops در نظر گرفته شوند.

ترکیب AIops با Generative AI

یکی از روندهای مهم سال‌های اخیر، ترکیب AIops با Generative AI و Large Language Models است.

در معماری سنتی، یک مدل ممکن است تنها یک Anomaly Score تولید کند. اما یک LLM می‌تواند نتایج چندین مدل و منبع داده را در کنار اطلاعات عملیاتی سازمان تحلیل کند و نتیجه را به زبان طبیعی توضیح دهد.

این قابلیت می‌تواند به‌خصوص در Incident Triage و تحلیل اولیه بسیار مفید باشد.

با این حال، LLM نباید به‌صورت خودکار و بدون کنترل به سیستم‌های حساس دسترسی اجرایی داشته باشد. Hallucination، اشتباه در استدلال و برداشت نادرست از Context می‌تواند باعث اجرای تصمیم نامناسب شود.

بهترین رویکرد در بسیاری از محیط‌های حساس، استفاده از LLM به‌عنوان ابزار Decision Support و نه مرجع مستقل تصمیم‌گیری است.

محدودیت‌های AI Ops

با وجود ظرفیت قابل توجه AI Ops، این فناوری راه‌حلی جادویی برای تمام مشکلات عملیات IT نیست.

مهم‌ترین محدودیت‌ها عبارت‌اند از:

نخست، کیفیت داده. بدون داده مناسب، حتی پیشرفته‌ترین الگوریتم‌ها نیز نمی‌توانند عملکرد مطلوبی داشته باشند.

دوم، تغییر دائمی محیط. مدل باید بتواند با تغییر معماری و رفتار سیستم سازگار شود.

سوم، False Positive. هشدارهای اشتباه زیاد می‌تواند خودشان به ایجاد Alert Fatigue منجر شوند.

چهارم، False Negative. عدم شناسایی یک Failure مهم می‌تواند پیامدهای جدی داشته باشد.

پنجم، پیچیدگی Integration میان ابزارهای Monitoring، Logging، ITSM و Automation.

ششم، هزینه ذخیره و پردازش حجم بالای Telemetry.

هفتم، ریسک Automation. اگر سیستم اقدام اصلاحی اشتباهی را اجرا کند، ممکن است دامنه Incident افزایش پیدا کند.

بنابراین پیاده‌سازی AI Ops باید مرحله‌ای، قابل ارزیابی و متناسب با سطح ریسک سازمان باشد.

آینده AI Ops

آینده AI Ops احتمالاً به سمت سیستم‌هایی حرکت خواهد کرد که تنها خطا را شناسایی نمی‌کنند، بلکه چرخه کامل مدیریت آن را تا حد زیادی خودکار می‌سازند.

می‌توان این تحول را به شکل زیر تصور کرد:

Monitoring → Observability → AI Ops → Predictive AI Ops → Autonomous Operations

در معماری‌های پیشرفته، سیستم می‌تواند به‌طور مداوم داده‌های زیرساخت را جمع‌آوری کند، وضعیت عادی را مدل کند، ناهنجاری را شناسایی کند، Failure را پیش‌بینی کند، علت احتمالی را پیدا کند، تأثیر آن را تخمین بزند، بهترین اقدام را پیشنهاد کند و در صورت وجود مجوز، اقدام اصلاحی را اجرا کند.

پس از اجرای اقدام نیز نتیجه باید دوباره به سیستم بازگردد تا عملکرد مدل و سیاست عملیاتی ارزیابی شود.

این مفهوم به **Closed-Loop IT Operations** نزدیک می‌شود؛ یعنی چرخه‌ای که در آن مشاهده، تحلیل، تصمیم و اقدام به‌صورت پیوسته انجام می‌شوند.

نتیجه‌گیری

AIOps را می‌توان یکی از مهم‌ترین رویکردهای نوین برای مدیریت پیچیدگی زیرساخت‌های فناوری اطلاعات دانست. افزایش تعداد سرویس‌ها، رشد معماری‌های توزیع‌شده، افزایش حجم Telemetry و کاهش امکان مدیریت دستی رخدادها باعث شده است که Monitoring سنتی به‌تنهایی برای بسیاری از سازمان‌های بزرگ کافی نباشد.

AIOps با ترکیب Metrics، Logs، Traces، Events، Topology و داده‌های ITSM با الگوریتم‌های یادگیری ماشین و هوش مصنوعی، امکان تشخیص ناهنجاری، پیش‌بینی Failure، همبستگی رخدادها، Root Cause Analysis و Automated Remediation را فراهم می‌کند.

با این حال، موفقیت AIops صرفاً به انتخاب یک الگوریتم پیچیده وابسته نیست. کیفیت داده، طراحی معماری، تعریف شاخص‌های مناسب، مدیریت Concept Drift، تفسیرپذیری، امنیت و کنترل Automation نقش بسیار مهمی دارند.

مهم‌تر از همه، AIops نباید به‌عنوان جایگزینی کامل برای متخصصان IT در نظر گرفته شود. ارزش اصلی این فناوری در افزایش توان تیم‌های عملیاتی، کاهش کارهای تکراری، کاهش Noise، سرعت بخشیدن به تشخیص و فراهم کردن امکان تصمیم‌گیری پیش‌نگرانه است.

در نهایت، بلوغ AIops زمانی محقق می‌شود که سازمان از مرحله «تشخیص خطا پس از وقوع» عبور کند و به مرحله «درک رفتار سیستم، پیش‌بینی Failure و اقدام پیشگیرانه» برسد. ترکیب AIops با Observability، Machine Learning، Graph Analytics، Generative AI و Automation می‌تواند زمینه ایجاد زیرساخت‌هایی را فراهم کند که نه تنها قابل مشاهده و مدیریت، بلکه پیش‌بین، هوشمند و تا حدی خودترمیم‌شونده باشند.

منابع

Notaro, P., Cardoso, J., & Gerndt, M. (۲۰۲۱). A survey of AIOps methods for failure management. ACM Transactions on Intelligent Systems and Technology, ۱۲(۶), Article ۸۱.

Remil, Y., Bendimerad, A., Mathonat, R., & Kaytoue, M. (۲۰۲۴). AIOps solutions for incident management: Technical guidelines and a comprehensive literature review. arXiv.

Zhong, Z., Fan, Q., Zhang, J., Ma, M., Zhang, S., Sun, Y., Lin, Q., & Pei, D. (۲۰۲۳). A survey of time series anomaly detection methods in the AIOps domain. arXiv.

Zhang, L., Jia, T., Jia, M., Wu, Y., Liu, A., Yang, Y., Wu, Z., Hu, X., Yu, P. S., & Li, Y. (۲۰۲۴). A survey of AIOps for failure management in the era of large language models. arXiv.

IBM. (۲۰۲۵). What is AIOps and how does it relate to observability? IBM Think.

Gartner. (۲۰۲۴). Solution criteria for AIOps platforms. Gartner Research.

Cisco. (۲۰۲۵). What is AIOps? Cisco.