# تغییر فناوری ها و روندها در سال 2024

## قسمت اول

**ترجمه :** تیم تحریریه ایکاست

اصطلاح "تحول دیجیتال" سال‌هاست که بر سر زبان‌هاست، بنابراین عمر مفید آن به سر رسیده باشد. با این حال، ظهور فناوری‌های نوظهور و بلوغ فناوری‌های عبور کرده از چرخه هیاهو، طوفان کاملی برای یک دگرگونی دیجیتال گسترده ایجاد کرده است. این اصطلاح آشنا در سال 2024 با ظهور اینترنت اشیای بالغ، نسل پنجم در حال توسعه، ملاحظات هوش مصنوعی و گزینه‌های اتصال فراگیر، جانی دوباره خواهد گرفت.

# اینترنت اشیا در عمودی و عمودی سازی اینترنت اشیا

در بحث اینترنت اشیاء(IoT) ، اغلب بین دو بعد افقی و عمودی تمایز قائل می شویم. "افقی" به تمام اجزای ساختاری یک راهکار IoT اشاره دارد، از جمله دستگاه ها، شبکه ها، پروتکل های ارتباطی و پلتفرم های ابری. شرکت هایی که این عناصر افقی را می فروشند، تمایل دارند از IoT به عنوان چتری گسترده یاد کنند که عناصر فناوری مختلفی را در خود جای داده است. اما این دیدگاه با دیدگاه "عمودی" متفاوت است. دیدگاه عمودی به نیازهای خاص مشتریان و کاربردهایی که قصد پیاده سازی آن را دارند، معطوف می شود. این موارد می تواند شامل مدیریت ناوگان، نگهداری پیش بینی برای تجهیزات کارخانه، کنتورهای هوشمند یا هر تعدادی از سایر موارد استفاده باشد. افراد در بخش عمودی به طور کلی به کاری که انجام می دهند به عنوان IoT فکر نمی کنند. آنها به مورد استفاده فکر می کنند. بنابراین، برای هر کسی که IoT را می فروشد، درک این موضوع که کاربران نهایی دنیا را به همان شکلی که آنها می بینند نمی بینند، بسیار مهم است. این همیشه مورد استفاده است که تقاضا را هدایت می کند، نه فناوری، و دنیای IoTباید بداند چگونه قابلیت های فناوری را در بستر مناسب قرار دهد. فناوری 5G جنبه جالبی دارد که امکان ارائه عملکردهایی خاص مانند کیفیت خدمات بالاتر، تاخیر کمتر یا قابلیت اطمینان بیشتر را فراهم می کند که برای انواع خاصی از پیاده سازی ها مانند اتوماسیون کارخانه یا خدمات اضطراری بسیار مفید خواهد بود. نکته کلیدی این است که قابلیت را در چارچوب نحوه استفاده مشتری از آن ارتباط دهیم. نه "اینترنت اشیاء" و حتی "5G" ، بلکه "مدیریت بلادرنگ" یا "اتصال تضمینی"

MATT HATTON Founding Partner, Transforma Insights

اینترنت اشیاء (IoT) همانند هر بخش دیگری در فناوری، در حال تحول مستمر است. مفهوم IoT که در ابتدا به عنوان ارتباط ماشین به ماشین (M2M) شناخته می‌شد، گسترش یافته و اکنون بر هر "چیزی" قابل اتصال به اینترنت دلالت می‌کند. راه‌حل‌های ارائه شده برای پشتیبانی از IoT عمدتاً "افقی" بودند، شامل سخت‌افزار، پلتفرم و اتصال.

با گسترش فراگیرتر IoT و ارتقای مستمر قابلیت‌های آن از طریق پیشرفت‌های فناوری جدید، فروش مجموعه‌ای گسترده از راه‌حل‌ها به بخش‌های مختلف بازار دیگر کافی نیست.

با توجه به نیازهای متفاوت بخش‌های عمودی درIoT ، رویکردهای متفاوتی نیز لازم است. زیرساختی که از یک اپلیکیشن "شهر هوشمند" پشتیبانی می‌کند، نمی‌تواند از یک راه‌حل "مراقبت‌های بهداشتی دیجیتال" حمایت کند.

عرضه‌های افقی در IoT همچنان حیاتی هستند و حتی اهمیت آن‌ها رو به افزایش است. در همین برگه سفید به بررسی تغییرات محیط در اتصال جهانی خواهیم پرداخت که این عنصر حیاتیIoT ، بر اجزای مختلف پشته IoT تأثیر می‌گذارد.

اما ارائه همان راه‌حل افقی به یک تولیدکننده که نیاز به سنسورهای صنعتی IoT برای تعمیر و نگهداری پیش‌بینی‌کننده دارد و یک شرکت حمل و نقل که می‌خواهد وسایل نقلیه خود را به دوربین‌های پیشرفته مجهز به هوش مصنوعی (AI) مجهز کند، کارآمد نخواهد بود.

سازمان‌ها باید راه‌حل‌ها و خدمات خود را با بازارهای عمودی تطبیق دهند و اجزای کلیدی مورد نیاز برای خدمت به این بازارها را درک کنند.

ارائه‌های افقی در اینترنت اشیاء همچنان حیاتی هستند و در واقع اهمیت آن‌ها رو به افزایش است. حتی همین برگه سفید به بررسی تغییر محیط در اتصال جهانی می‌پردازد که این عنصر حیاتی IoT، بر بسیاری از اجزای پشته IoT تأثیر می‌گذارد.

## هوش مصنوعی: چرخه هایپ

در حالی که خود هوش مصنوعی و اینترنت اشیاء به تنهایی تاثیرگذار هستند، ما معتقدیم که زمانی که آن‌ها با هم ترکیب می شوند، زمانی که اکوسیستم ها و قابلیت های آنها همگرا می شوند، آن زمان است که به طور واقعی دستخوش تحول می شوند. ترکیب این فناوری ها، سناریویی را ایجاد می کند که در آن می توانید مقدار غیرقابل تصوری از داده را جمع آوری کرده و بدون دخالت انسان، پاسخ های تاثیرگذاری را برای این داده ها باز کنید. ما شاهد هستیم که این راه حل ها در طیف وسیعی از تنظیمات، از فروشگاه های خرده فروشی گرفته تا کف کارخانه ها و تا ماشین هایی که رانندگی می کنیم، اجرا می شوند، این همگرایی در حال رخ دادن است."

**JOSH BUILTA Director of IoT Research, Omdia**

نیمه دوم سال 2023 شاهد بحث های زیادی در مورد هوش مصنوعی و تأثیر آن بر فناوری، تجارت و جامعه بود. با ادامه این گفتمان، کشمکشی بر سر این موضوع به وجود آمده است که آیا هوش مصنوعی به یک فناوری پیشرو تبدیل خواهد شد که جایگزین سایر فناوری ها شود یا به عنوان یک فناوری همراه، از زیرساخت قوی و اکوسیستم موجود پشتیبانی خواهد کرد.

دامنه کاربرد هوش مصنوعی می تواند در سطوح مختلف باشد، از فعالیت های رویه ای مانند تشخیص چهره در فرودگاه ها تا حوزه گسترده ای مانند رباتیک در تولید، مراقبت های بهداشتی و غیره. برخی از قدیمی ترین کاربردهای هوش مصنوعی به راه حل های مبتنی بر پردازش تصویر تعلق دارند. به عنوان مثال، دوربین های مجهز به هوش مصنوعی در تلماتیک به اسکن تصویری هم داخل و هم خارج کابین کامیون اجازه می دهند. خروج ناایمن از خطوط یا پیچیدن تند می تواند به راننده هشدار داده شود و بدین ترتیب از راننده، وسیله نقلیه و بار محافظت شود. در داخل کابین، رفتار راننده برای شناسایی و جلوگیری از رفتارهای ناایمن مانند استفاده از تلفن همراه یا خستگی کنترل می شود. به راننده به صورت بلادرنگ از طریق سیستم داخل کابین هشدار داده می شود و ویدیو برای آموزش بیشتر به مدیر ناوگان ارسال می شود.

فرصت‌های تلماتیک دیگری می‌تواند دید واضح‌تری از نحوه حرکت کامیون‌های ناوگان ارائه دهد. حصارکشی جغرافیایی به طور سنتی رویکردی برای نظارت بر نحوه خروج کامیون ها از پارکینگ یا رسیدن به مقصد تحویل بوده است، اما نیازمند نقشه برداری دستی اولیه است. با دوربین‌های هوش مصنوعی، کامیون‌ها می‌توانند از میدان دید دوربین عبور کنند - مانند عبور از یک پارکینگ محصور - و دوربین زمان، تاریخ، مکان و خودروی دقیق را ثبت می‌کند. همانطور که قبلاً ذکر شد، سیستم های دوربین شناسایی چهره در فرودگاه ها نیز فرصتی برای کاهش فشار بر نیروی کار و ایجاد کارایی بیشتر برای مسافران است.

یادگیری ماشین (ML) یکی از زیرمجموعه‌های هوش مصنوعی (AI) است که تمرکز بیشتری بر روش‌های الگوریتمی پردازش داده دارد، در حالی که هوش مصنوعی بیشتر به سمت انجام کارها به صورتی شبیه به انسان است.

برخی معتقدند که هیاهوی پیرامون هوش مصنوعی توجه به قدرت یادگیری ماشین و دستاوردهای آن برای سازمان‌ها از طریق بهینه‌سازی، کاهش خطا و غیره را تحت‌الشعاع قرار داده است. یادگیری ماشین این امکان را به ماشین‌ها می‌دهد که با استفاده از الگوریتم‌ها آموزش ببینند و با معرفی داده‌های جدید خود را اصلاح کنند، اما این محدودیت منطق آن است. در بسیاری از موارد استفاده، این قابلیت قدرتمند و انقلابی است. در چنین مواردی، پیش بردن آن به سطح هوش مصنوعی صرفاً ارزش افزوده‌ای ایجاد نمی‌کند. بنابراین سوال این است که آیا صرفاً به دلیل توانایی هوش مصنوعی، باید از آن استفاده کرد؟

ارائه دهندگان خدمات اتصال در حال حاضر شاهد پیاده سازی گسترده یادگیری ماشین در طیف وسیعی از کاربردها هستند. از یک سو، این الگوریتم ها برای درک رفتار غیرعادی سیم کارت ها و دستگاه ها در شبکه به کار گرفته می شوند که به مشتریان و ارائه دهندگان خدمات امکان می دهد به موقع اقدامات لازم را انجام دهند.

به تازگی، شاهد استفاده از ابزارهایی مانند هوش مصنوعی تولیدکننده هستیم که به کاربران کمک می کند بدون نیاز به تخصص تحلیلی، الگوهای رفتاری دستگاه ها را از طریق نمایش به زبان طبیعی درک کنند. در آینده، این نوع موارد استفاده به سیستم های حلقه بسته گسترش خواهند یافت، که در آن از یادگیری ماشین یا هوش مصنوعی برای درک زمینه ها و الزامات استفاده می شود و به جای هشدار دادن صرف به کاربران در مورد رویدادهای خاص، اقدامات خودکار برای بهینه سازی مدیریت دستگاه ها انجام می شود. با افزایش حجم و پیچیدگی سیم کارت های مشتریان، این امر به یک تمایز واقعی در کاهش چالش های مدیریت تبدیل خواهد شد.

بر اساس نظرسنجی های IoT سازمانی ما، می دانیم که بسیاری از شرکت ها خواهان یک راه حل خدمات اتصال کاملاً مدیریت شده هستند، اما هزینه ها مانعی بر سر راه است. یادگیری ماشین یا هوش مصنوعی ممکن است با هزینه های سربار کمتری که معمولاً با چنین رویکرد راهبردی همراه است، مسیر جدیدی به سمت این هدف ایجاد کند.

**STEFFEN SORRELL Chief of Research, Kaleido Intelligence**

سیستم های هوش مصنوعی برای عملکرد به اتصالی پایدار و قوی سلولار وابسته هستند. با این حال، چنین اتصالی همیشه در سراسر جهان در دسترس نیست. در حالی که اپراتورهای تلفن همراه (MNO)، ارائه دهندگان خدمات اینترنت اشیاء (IoT) و تولیدکنندگان دستگاه های هوش مصنوعی متصل به اینترنت اشیاء برای ارائه اتصالی مطمئن تلاش می کنند، همچنان در راستای توانمندسازی قابلیت های هوش مصنوعی و یادگیری ماشین در دستگاه های اینترنت اشیاء وابسته به اینترنت سلولی، جای پیشرفت وجود دارد. یکی از راه حل های پیشنهادی استفاده از سیم کارت های multi-IMSI می باشد که با اتصال همزمان به چند شبکه، اطمینان از اتصال دائمی را فراهم می کند.

## چالش و نیاز: امنیت، حاکمیت و انطباق

همانطور که جهان ما به سمت ارتباطی فراگیر حرکت می کند، شاهد تغییری قابل توجه در صنعت هستیم. صحبت در مورد امنیت بیشتر می شود و من معتقدم شاهد تغییری خواهیم بود که در آن مسئولیت ایمن سازی راه حل های دیجیتال کمتر بر دوش مشتریان و بیشتر بر روی ارائه دهندگان زیرساخت قرار خواهد گرفت. به طور واضح مشخص شده است که وظیفه اصلی بازیگران زیرساخت، حفاظت از کل اکوسیستم، از جمله اپراتورهای تلفن همراه، اپراتورهای مجازی تلفن همراه و مشتریان سازمانی است، چه به طور مستقیم و چه غیرمستقیم. مهمترین وظیفه، حفاظت از کل زنجیره از دستگاه ها از طریق شبکه و انتقال داده ها به برنامه ("دستگاه به ابر") است. نتیجه این امر، اقدامات امنیتی مبتنی بر شبکه خواهد بود که مشتریان را با امنیت سطح دستگاه، درگیر نکند. هزینه‌های دستگاه‌ها در حال کاهش است که منجر به استفاده تولیدکنندگان از مودم‌های پیچیدگی پایین‌تر می‌شود که به اندازه مودم‌های گوشی‌های هوشمند قوی نیستند. این امر توانایی پشتیبانی از ویژگی‌های امنیتی اضافی مانند رمزگذاری و VPN ها را کاهش می‌دهد، بنابراین امنیت قوی‌تر شبکه را ضروری می سازد. مدلی که به آن نیاز داریم - و آنچه که در آغاز سال 2024 به سمت آن در حال حرکت هستیم - اطمینان می دهد که شبکه ها به اندازه ای امن هستند که بتوانند داده ها را از دستگاه به ابر به روشی ایمن، کارآمد و یکپارچه انتقال دهند. مشتریانی که اقدامات امنیتی خود را دارند باید بتوانند آنها را با ارائه دهندگان زیرساخت ادغام کنند. به جای مواجهه با موانع در ادغام، شبکه‌ها – مانند floLIVE – باید باز، شفاف و یکپارچه باشند تا به مشتریان یا اقدامات امنیتی شخص ثالث ما اجازه دهند تا به طور یکپارچه متصل شوند.

**NIR SHALOM floLIVE, CEO**

با افزایش استفاده از دستگاه‌های اینترنت اشیاء، نگرانی‌های امنیتی و همچنین چالش‌های مربوط به محل نگهداری داده‌ها نیز افزایش می‌یابد. انتظار می‌رود که در سال جاری شاهد پیشرفت‌های بیشتری در نحوه انجام امنیت و همچنین افزایش چالش‌ها با حاکمیت داده‌ها و چگونگی انطباق با قوانین و مقررات باشیم.

## امنیت سخت افزار و اعتماد صفر(Hardware security and Zero trust)

هنگامی که انواع مختلفی از دستگاه ها را برای انتقال داده های مهم به اینترنت متصل می کنیم، خطر ذاتی است.
یکی از بزرگترین چالش ها در امنیت دیجیتال، سخت افزار است. با رشد بازار راه حل های دیجیتال، دستگاه های سخت افزاری بیشتری وارد بازار می شوند، اما به دلیل محدودیت های مالی یا تجربی، ممکن است امنیت دستگاه ها برای همه تولیدکنندگان در اولویت نباشد. دستگاه های سخت افزاری با سیستم عامل منسوخ، رمزگذاری ناکافی، دسترسی محلی ناامن، عدم تغییر رمزهای عبور پیش فرض و آسیب پذیری در سفارشی سازی مورد تهدید قرار می گیرند.
تنها با بررسی سه ماهه دوم سال 2023، 66 درصد از ماژول های اینترنت اشیاء سلولی ارسال شده هیچ امنیت سخت افزاری اختصاصی نداشتند و 29 درصد هیچ ویژگی امنیتی نداشتند.

یک رویکرد نوظهور در امنیت سطح دستگاه، IoT SAFE (اپلیکیشن سیم کارت IoT برای ارتباط امن End-to-End) است که از سیم کارت به عنوان عنصر امنیتی سخت افزاری، که به عنوان "Root of Trust" نیز شناخته می شود، استفاده می کند.
با این کار، امنیت تراشه به ابر به روشی ساده ایجاد می شود، زیرا همه دستگاه ها به سیم کارت نیاز دارند. ادغام امنیت هنگام استفاده از سیم کارت، به طور خودکار دستگاه را به امنیت سطح سخت افزار مجهز می کند و IoT SAFE برای همه فرم های سیم کارت مناسب است که از قفل شدن با یک فناوری خاص جلوگیری می کند.

بر اساس GSMA، IoT SAFE امنیت را با فعال کردن موارد زیر به دست می آورد:

- امکان احراز هویت متقابل (D)TLS امن دستگاه های IoT به یک سرور با استفاده از طرح های امنیتی نامتقارن یا متقارن.
- توانایی محاسبه اسرار مشترک توسط دستگاه های IoT و محرمانه نگه داشتن کلیدهای بلند مدت.
- مدیریت تدارکات و چرخه عمر اعتبارنامه از یک سرویس امنیتی IoT از راه دور.

IoT SAFE رویکردی است که به سمت یک مدل امنیتی مدرن تر و بدون اعتماد برای اینترنت اشیاء کار می کند. همانطور که مایکروسافت توضیح می دهد، دستگاه های اینترنت اشیاء با چالش های امنیتی منحصر به فردی مواجه هستند، از جمله:

- عدم وجود امنیت از همان ابتدا
- مشکلات ادغام با زیرساخت‌های امنیتی موجود
- آسیب‌پذیری‌های امنیتی بالقوه بالا
- قرار گرفتن در معرض خطر بیشتر به دلیل مکان فیزیکی

مدل امنیتی بدون اعتماد به طور کامل این خطرات را پذیرفته و انتظار تهدید را دارد. این مدل از احراز هویت قوی، به‌روزرسانی‌های OTA برای دستگاه‌های سالم و نظارت دقیق پشتیبانی می‌کند.

## محلی سازی داده ها

با تبدیل شدن استفاده از داده به رکن اصلی عملیات، حاکمیت داده به موضوعی داغ تبدیل شده است. ابر در نحوه پردازش و ذخیره داده ها انقلابی ایجاد کرده است و به محاسبات توزیع شده اجازه می دهد تا رونقی در راه حل های دیجیتال ایجاد کند.
خدمات و راهکارهای مبتنی بر رایانش ابری، معماری و نرم افزار به گونه ای غیرمتمرکز شده اند که داده ها در آن پردازش و نگهداری می شوند. سرمایه گذاری های سنگین گذشته در مراکز داده، که ریسک مبتنی بر بازگشت سرمایه را در پروژه های مبتنی بر داده ایجاد می کرد، دیگر وجود ندارد.
آزادی استفاده از ابر به سازمان ها اجازه داد تا به سرعت راه حل های دیجیتال را با هزینه کمتر، مدیریت کمتر و آزادی بیشتر مقیاس بندی کنند. ظهور غول های ابر (Hyperscaler)در دهه گذشته اکنون گفتگویی را درباره محل نگهداری داده ها آغاز کرده است. آیا یک سازمان مستقر در استرالیا که از یک ابر بزرگ در ایالات متحده استفاده می کند، باید محل تایید شده خود را به این ابر بزرگ منتقل کند؟
حریم خصوصی داده ها و امنیت سایبری بازیگران مهمی در حاکمیت داده ها و مقررات مربوطه هستند که پیشنهاد و/یا به عنوان قانون الزامی می شوند. این چشم انداز به طور منظم در حال تغییر است و با ظهور موارد استفاده با نیاز شدید به داده بیشتر ( هوش مصنوعی و یادگیری ماشینی)، حاکمیت داده ها توجه بیشتری را به خود جلب می کند.
ابر و محاسبات را می توان به طرق مختلف تقسیم و غیرمتمرکز کرد. پیچیدگی زیرساخت ابری می تواند حاکمیت داده ها را پیچیده کند، اما یکی از رویکردهای کلیدی برای رعایت مقررات محلی، محاسبات لبه (Edge Computing) است.

## تعریف لبه(Defining the Edge)

مفهوم لبه مدت زیادی با ما بوده است و در واقع، قبل از ظهور رایانش ابری وجود داشته است. فناوری های لبه امروزه همچنان بسیار مرتبط هستند و با افزایش تقاضا برای برنامه های مبتنی بر اینترنت اشیا و هوش مصنوعی "حاشیه ای"، اهمیت آنها بیشتر می شود. فناوری های لبه پاسخ های کم تاخیر به رویدادهای محلی حس شده توسط دستگاه های اینترنت اشیاء را امکان پذیر می کنند و با حفظ پردازش محلی، مزایایی مانند اجتناب از هزینه های ارتباطی برای انتقال داده ها به ابر، افزایش انعطاف پذیری و توانایی ادامه عملکرد در صورت خرابی اتصال در مناطق وسیع، و حفظ حریم خصوصی و مالکیت داده ها را ارائه می دهند. فناوری های لبه اغلب برای برنامه های اینترنت اشیاء که از قابلیت های هوش مصنوعی نیز در یک راه حل استفاده می کنند، بسیار مهم هستند و ما انتظار داریم که در سال های آینده تعداد زیادی از این نوع برنامه ها وجود داشته باشد. با این حال، فناوری های لبه یک داروی جهانی نیستند. به احتمال زیاد، راه حل های اینترنت اشیاء مانند آلارم ها و محرک های اولیه، و به ویژه آنهایی که به عمر باتری طولانی نیاز دارند، هرگز از فناوری هایی که امروزه به عنوان لبه شناخته می شوند استفاده نمی کنند، زیرا مصرف انرژی کم در چنین زمینه هایی بسیار مهم است.

**JIM MORRISH Founding Partner, Transforma Insights**

ایده محاسبات نزدیک به سطح دستگاه، یک مفهوم جدید نیست و در واقع، همان روشی است که پردازش اولیه داده ها انجام می شد. با ظهور اینترنت، محاسبات توزیع شده به سمت سرورها و سپس با افزایش تقاضای داده به سمت ابر منتقل شدند. با گسترش مداوم حجم داده ها، مسئله تاخیر، جزر و مد را به سمت پردازش نزدیک به سطح دستگاه بازگردانده است.
این کار نه تنها می تواند تاخیر را کاهش داده و عملکرد را بهبود بخشد، بلکه می تواند هزینه عملیاتی مرتبط با میزبانی ابری را نیز کاهش دهد و به سازمان مالکیت و کنترل بیشتری بدهد.

علاوه بر این، با اجرای مدل های هوش مصنوعی و یادگیری ماشین در لبه، برنامه های بلادرنگ می توانند از پیشرفت های چشمگیری بهره مند شوند. این امر امکان ارائه خدمات و کسب و کارهای جدید را فراهم می کند و دیجیتالی کردن برنامه های مدرن که نیاز به پردازش مقادیر بیشتری از داده ها، حتی زمانی که حاوی رسانه های غنی هستند، را ممکن می سازد.
برای مثال، در یک برنامه سازمانی، مقادیر عظیمی از داده های لبه را می توان برای پردازش لحظه ای از طریق مدل های هوش مصنوعی و الگوریتم های یادگیری ماشین اجرا کرد. برای دستگاه های اینترنت اشیاء که از هوش مصنوعی / یادگیری ماشین استفاده می کنند، اتصال متناسب با لبه محاسباتی ضروری است. اعتقاد بر این است که شبکه های سلولی جهانی که از چندین هسته اصلی استراتژیک در سراسر جهان استفاده می کنند، می توانند به پردازش سریعتر داده نزدیک به منبع کمک کنند.

توسعه لبه برای دستگاه های اینترنت اشیاء، به ویژه در دستگاه های کوچک کم مصرف با توان پردازشی محدود، ضروری است. این معماری زمان پاسخ سریع‌تر، حریم خصوصی داده‌های بهتر، امنیت و انعطاف‌پذیری بیشتری در نبود اتصال به ابر ارائه می‌کند - و آن را برای دستگاه‌های حیاتی ایده‌آل می‌کند. با این حال، اجرای اتصال امن به دلیل محدودیت توان پردازشی یک چالش است، که این دستگاه‌ها را آسیب‌پذیر می‌کند، که برای دستگاه‌های حیاتی قابل قبول نیست.
یکی از راه‌حل‌های بالقوه برای رفع این آسیب‌پذیری، استفاده از سیم‌کارت‌های هوشمند است که قادر به احراز هویت با ابر با بیشترین امنیت ممکن هستند.

**VERA MIRETSKY Vice President of R&D, FloLIVE**

با افزایش قدرت پردازش، رشد تقاضا برای راه‌حل‌های دیجیتالی و لزوم توزیع بار داده‌ها بین منابع مختلف، محاسبات لبه می‌تواند برای بهبود برنامه‌های کاربردی دیجیتال در صنایع مختلف مورد استفاده قرار گیرد.

**با این حال، همه رویکردهای لبه یکسان نیستند و تا حد زیادی به مورد استفاده بستگی دارند. دو مورد از رایج ترین حوزه های مرتبط با لبه عبارتند از:**

- **لبه دستگاه:** این روش برای مواردی مناسب است که نیاز به تاخیر کم و کاهش ترافیک برگشتی وجود داشته باشد و در آن بار کاری مستقیماً روی سخت افزار فیزیکی اجرا شود.
- **محاسبات لبه محل:** این روش به دروازه اینترنت اشیا که به صورت فیزیکی در محل یا مرکز داده داخلی قرار دارد اشاره می کند. این روش برای مواردی مناسب است که حفظ داده های حساس در محل مورد نظر است.

این رویکرد "ابر توزیع شده" باعث بومی سازی محل پردازش و نگهداری داده ها می شود، اما همچنان امکان مدیریت زیرساخت را فراهم می کند و مسئولیت کلی همچنان بر عهده ارائه دهنده خدمات ابری است.

مرجع :FLOLIVE.NET

**تماس با ما:**

**شرکت عصر ارتباطات بین الملل پارس کار (ایکاست)**

**آدرس : تهران، سعادت آباد، میدان بهرود، خیابان عابدی، پلاک 15، ساختمان صبا، طبقه سوم واحد 8**

**کد پستی : 1981863695**

**تلفن : +98-21-75-229-229**

**فکس : +98-21-75-229-239**

**وبگاه : www.icasat.net**

**پست الکترونیک : crm@icasat.net**