IoT-trender 2025: Säkerhet, hållbarhet och AI

PQC och Zero Trust är två strategier för cybersäkerhet.

EXPERTARTIKEL

Av Ulf Seijmer, Induo och AKKR8

Ulf Seijmer är innovationschef på Induo samt CTO och medgrundare till hårdvaruföretaget AKKR8. Han är också styrelsemedlem i EUTECHs IoT Alliance. År 2012 skrev han en av de första artiklarna om 5G, en artikel som publicerades i Elektroniktidningen. Ulf är en frekvent anlitad föreläsare inom trådlös teknik för LPWAN och 5G.

Termen "The Internet of Things" (IoT) lär ha myntats av den brittiska teknikpionjären och datavetaren Kevin Ashton 1999. Om så är fallet, ja då fyllde IoT 25 år förra året, och det är helt klart en milstolpe som passerats, men IoT-resan har väl bara börjat? IoT fortsätter att transformera både företag och samhället. I omvärlden identifierar vi tre starka trender – hållbarhet, säkerhet och AI som kommer att fortsätta forma området. IoT utvecklas från att vara en teknisk lösning till en strategisk nödvändighet för företag och organisationer.

Ökat klimatansvar driver beslutsfattande

Hållbarhet är i dag en av de mest framträdande trenderna inom IoT och är också en av de främsta anledningarna att företag investerar i IoT-lösningar, helt enligt övriga trender i samhället.

För större företag blir hållbarhetsrapportering allt viktigare, och IoT erbjuder möjligheter att samla data på ett systematiskt sätt. Genom att utnyttja IoT för kontinuerlig optimering kan företag inte bara förbättra sina processer utan också spåra sin hållbarhetspåverkan på ett sätt som tidigare inte var möjligt. Med ökande fokus på hållbarhet och ett ökat klimatansvar kommer IoT att spela en allt viktigare roll för företag som vill göra en mätbar skillnad.

Smarta lösningar kan idag inte bara mäta mängden avfall ett företag genererar utan även hur rent avfallet är med hjälp av AI och kameror. Sensorer och IoT-system gör det enklare att uppfylla allt striktare krav på hållbarhetsarbete och uppföljning av klimatpåverkan, samt att dokumentera och presentera konkreta resultat för intressenter och myndigheter. IoT-lösningar kan ge oss insikter om nuläget och när vi satt våra hållbarhetsmål tala om för oss om vi nått dem.

Säkerhet blir obligatorisk

I takt med att användningen av IoT växer blir frågan om säkerhet allt viktigare. Antalet malware-attacker mot IoT-enheter har ökat med 400 procent enligt Zscaler ThreatLabz, och detta är siffror från 2023. Trenden visar att dessa system blir allt mer intressanta att attackera. Utvecklingen leder till att nya globala säkerhetsstandarder och regelverk införs för att skydda både användare och system. EU har nya regelverk för cybersäkerhet, där bland annat RED-direktivet uppdateras med cybersäkerhetskrav. Från augusti 2025 måste alltså IoT-enheter möta cybersäkerhetskrav för att få säljas i EU. Det är inte bara här det händer, vi ser samma utveckling över hela världen. Nya standarder och regelverk skickar ett tydligt budskap om att säkerhet måste byggas in i varje IoT-enhet och plattform för att skydda användare mot potentiella hot och intrång.

Ytterligare tips på vägen

Två tips för framtiden, håll koll på PQC och Zero Trust. Postkvantkryptografi (PQC) erbjuder skydd mot hot som kan uppstå från kvantdatorer, vilket är relevant då framtida kvantdatorer kan knäcka dagens krypteringsstandarder snabbt. Genom att börja arbeta med PQC nu kan företag säkerställa att IoT-infrastrukturen är förberedd för säkerhetsutmaningen som kvantdatorer medför. Förvånansvärt många företag har enheter med användarnamn och lösenord som enda autentiseringsmetoder för att skicka data via öppna nät, ganska sannolikt så är dessa lätta

att knäcka med teknik som finns runt hörnet.

En annan viktig säkerhetsdisciplin som blir allt vanligare inom IoT är ”Zero Trust”. Istället för att anta att allt inom ett nätverk eller en konstruktion är pålitligt bygger Zero Trust på principen att ingenting och ingen implicit skall litas på. Varje åtkomstbegäran måste verifieras och godkännas, vilket skapar en betydligt säkrare miljö för IoT-applikationer och minimerar risken för attacker.

AI och IoT – livslångt partnerskap?

Den kanske mest omdanande utvecklingen inom IoT är AI:s inträde och det kommer inte att mattas av 2025. IoT kan generera enorma mängder av data som AI effektivt kan analysera. Genom att kombinera AI och IoT (AIoT) kan vi inte bara öka noggrannheten och effektiviteten hos de tjänster som levereras utan också förbättra säkerheten genom bättre analyser och insikter. AI används också för att identifiera säkerhetsluckor eller upptäcka avvikelser i IoT-nätverk i realtid. På detta sätt fungerar AI inte bara som en motor för dataanalys inom IoT, utan också som ett kraftfullt verktyg för att skydda och säkra IoT-system mot hot och sårbarheter.

Edge-intelligens och AI

AI:s integration i IoT går långt bortom traditionell dataanalys – vi ser nu att AI tar sikte på att bli en integrerad del av IoT-enheter, vilket gör det möjligt för enkla IoT-enheter att fatta smartare beslut lokalt.

Edge-computing eller edge-processing adresserar begränsningarna med centraliserade molnlösningar. Genom lokal databehandling nära datakällan kan fördröjningar och latens minimeras, vilket är avgörande för applikationer som behöver fungera utan störningar och med korta svarstider. Exempelvis självstyrande fordon eller industriell automation är områden som kräver hög tillförlitlighet och motståndskraft. I tillämpningar som smarta städer, där sensornätverk styr trafikljus eller övervakar luftkvalitet, kan lokala AI-algoritmer snabbt bearbeta data och agera utan att vara beroende av eller belasta centrala servrar. Detta är dessutom värdefullt för energieffektiviteten, då bearbetningen sker nära källan och mindre energi används för datatransport. Å andra sidan kan inte enheterna drivas på batteri då högre energiåtgång krävs för edge-computing än i en sensor som ”bara” mäter och skickar data vidare.

Säkerhet är också ett framträdande skäl att satsa på att behandla data lokalt istället för i molnet, då mindre data behöver överföras via nätverket och systemen kan fungera även vid störningar. Lokalt bearbetad data kan reducera risken för breda cyberattacker eller dataläckor. Exempelvis hade Volkswagen nyligen en läcka där data från 800 000 fordon, bland annat detaljerad GPS-position, fanns samlad i klartext i en AWS-plattform, där lösenordet fanns lagrat på ett lättillgängligt ställe. Hade data behandlats i fordonet och inte skickats vidare så hade inte

Under 2025 kommer många LPWAN-tekniker att börja ta hjälp av satelliter.

stora mängder data samlats på en plats. IoT-plattformar som AWS IoT Greengrass V2 och Azure IoT Edge möjliggör hybridmodeller där kritiska processer hanteras nära enheterna medan molnet används för central analys och långsiktig lagring.

För organisationer som vill optimera prestanda och säkerhet utan att offra skalbarhet ger edge computing möjligheten att möta IoT:s utmaningar i moderna digitaliseringsprojekt. Edge computing passar särskilt bra för distribuerade AI-system som kräver decentraliserade beslut men trots fördelarna måste man också väga in dess begränsningar. Edge är inte alltid lämpligt för att hantera komplexa modeller som kräver uppdateringar från centraliserade datakällor. AI-modeller tränas ofta på insamlad data, vilket edge-system sällan kan hantera. Dessutom saknar mindre edge-enheter ofta tillgång till avancerade resurser som GPU-acceleration, vilket gör att beräkningstunga processer blir mindre effektiva om de utförs lokalt jämfört med ett datacenter.

Ju mer vi vill att edge-enheter skall hantera desto högre hårdvarukostnad, därför bör lokal AI i en enklare IoT-enhet i dagsläget ses som en möjlig förstärkning snarare än en ersättning för molnbaserad AI. Ett hybrid-upplägg som kombinerar realtidsfördelarna med edge och storskalig analyskraft i molnet ger ett balanserat och flexibelt AI-ekosystem som kan möta både lokala och globala databehandlingsbehov.

Vad händer i luften då?

Jag har tidigare skrivit en artikel för Elektroniktidningen om olika trådlösa tekniker för IoT. Under 2025 kommer många LPWAN-tekniker att förbereda sig att flytta ut i rymden. Så kallade NTN-nätverk, Non-terrestrial Networks, är basstationer som flygs i omloppsbana runt jorden och kan täcka alla världens hörn. Både LoRaWAN och 5G kan fungera via satellit och system är redan igång. 5G kan sedan en tid använda satelliter som RF-repeater där satelliterna saknar möjlighet att avkoda paket, medan de i kommande uppdateringar av 5G kan ta emot och vidareförmedla datapaket. Under 2025 är det sannolikt att andra LPWAN RF-tekniker som exempelvis Mioty tar sig ut i rymden. Även Starlink lanserar 2025 IoT från satelliter, dock med LTE CAT-1, CAT-1 Bis och CAT-4-teknik, vilket är 4G snarare än LPWAN-teknik (alltså inte ”Low Power”).

Om vi håller oss på jorden så är min spaning att 5G RedCap (Reduced Capacity) kommer att få ett större fäste. RedCap är litet som mellanmjölk, den är inte snabbast, den är inte strömsnålast, men den erbjuder runt 150 Mbit/s och är avsedd för litet mer krävande typer av sensorer. RedCap kan bli tekniken som kapacitetsmässigt kan försörja nästa generations sensorer med stabil uppkoppling. Den klarar både de frekvenser som används för privata 5G-nät, där inte nuvarande 3GPP LPWAN tekniker (NB-IoT och LTE-M) inte fungerar. RedCap erbjuder både korta svarstider och bra överföringshastighet, så i de sammanhang där sensorer ska processa mycket data lokalt, och kanske förses med AI och dessutom fungera i litet mer krävande miljöer, ja då tycker jag RedCap fyller sitt syfte.

LoRaWAN då? Cisco meddelade sent 2024 att de kommer att lämna LoRaWAN-marknaden. Från 2025 säljer företaget inte längre LoRaWAN-produkter och lagom till 2030 upphör supporten. Befintliga kunder behöver söka alternativa leverantörer för att säkerställa kontinuitet. Bortsett från det så verkar LoRaWAN som teknik följa trender och utveckling på IoT-marknaden och pratar om ökad grad av kryptering, bättre stöd för fjärruppdatering av mjukvara och möjlighet till lokal AI-behandling av data. En del av dessa koncept för dock LoRaWAN från en ren LPWAN-teknik med batteridrift närmare mer energikrävande hårdvara.

En ljus framtid hägrar

IoT som term fyllde alltså nyligen 25 och för mig är IoT ett teknikassisterat beslutsfattande baserad på verkliga data med potential att öka effektiviteten, minska kostnaderna och minimera miljöpåverkan. En sak är säker, behovet av IoT kommer inte att ebba ut i närtid. Med hållbarhet, säkerhet och AI i fokus står IoT redo att revolutionera både företag och samhället. Med en väl avvägd balans mellan innovation och säkerhet kan vi se fram emot en framtid där IoT inte bara är tekniskt imponerande utan även praktiskt och ansvarsfullt integrerat i våra dagliga liv. ■