

IoT Menggunakan LAN dan WAN

Internet of Things (IoT) merupakan konsep jaringan global di mana perangkat fisik seperti sensor, aktuator, dan objek sehari-hari dilengkapi konektivitas internet sehingga dapat saling berkomunikasi otomatis. Mansour et al. (2023) mendefinisikan IoT sebagai “jaringan global perangkat yang saling terhubung untuk bertukar data.” Dengan IoT, objek pasif dapat berubah menjadi perangkat cerdas yang mampu mengirim dan memproses informasi secara real-time. Gerodimos et al. (2023) menambahkan bahwa sensor membuat objek “mampu berkomunikasi data waktu nyata sehingga meningkatkan efisiensi dan membuat lingkungan lebih cerdas dan responsif.”

IoT kini berkembang pesat karena dukungan teknologi seperti chipset murah, jaringan nirkabel ubiquitous, kecerdasan buatan, serta 5G. Dauda et al. (2024) menekankan bahwa IoT merupakan bidang strategis dengan aplikasi luas: mulai dari kesehatan, transportasi, industri, hingga rumah tangga. Ekosistem ini diprediksi mencakup miliaran perangkat dalam dekade mendatang, menjadikannya fondasi transformasi digital global.

Dalam arsitektur IoT, jaringan menjadi elemen kunci. Data dari perangkat biasanya dikumpulkan di gateway atau LAN lalu diteruskan ke layanan cloud melalui WAN. Mansour et al. (2023) menjelaskan bahwa “lapisan gateway mengandung data jaringan seperti LAN dan WAN” untuk kemudian diolah di awan. Almutairi dan Sheldon (2025) menambahkan bahwa jaringan IoT melibatkan LAN, WAN, jaringan seluler, serta protokol khusus seperti Zigbee, 6LoWPAN, dan LoRa. LAN digunakan untuk menghubungkan perangkat dalam area terbatas (rumah, kantor, pabrik) menggunakan Wi-Fi, Ethernet, atau mesh. Sebaliknya, WAN mencakup area luas melalui internet, jaringan seluler (NB-IoT, LTE), maupun LPWAN (LoRaWAN) agar perangkat terhubung ke cloud.

Kelebihan LAN antara lain bandwidth tinggi, latensi rendah, serta biaya relatif murah di area terbatas. Hal ini menjadikannya cocok untuk aplikasi real-time seperti rumah pintar atau pabrik otomatis, di mana sensor dan aktuator harus saling terhubung cepat. Namun jangkauannya terbatas hanya puluhan hingga ratusan meter. LAN juga bisa mengalami interferensi nirkabel atau peningkatan beban jaringan saat banyak perangkat terhubung.

WAN, di sisi lain, menawarkan jangkauan sangat luas. Dengan internet publik, jaringan seluler, atau LPWAN, perangkat dapat berkomunikasi dari lokasi terpencil. LoRaWAN dapat menjangkau puluhan kilometer dengan daya rendah, sementara NB-IoT memanfaatkan infrastruktur seluler untuk konektivitas hemat energi. Teknologi ini memungkinkan aplikasi seperti pertanian cerdas (sensor tanah di ladang luas) dan kota cerdas (sensor polusi di banyak titik). Kekurangannya, WAN memiliki throughput rendah, latensi lebih tinggi dibanding LAN, serta biaya tambahan karena bergantung pada operator seluler atau infrastruktur khusus.

Dalam praktiknya, LAN dan WAN digunakan bersamaan. Rumah pintar biasanya memakai LAN (Wi-Fi, Zigbee) agar perangkat saling terhubung lokal dengan cepat. Jika pemilik ingin mengontrol dari luar rumah, data diteruskan ke cloud melalui WAN. Pada pertanian cerdas, sensor tanah mengirim data ke cloud lewat LoRaWAN atau NB-IoT. Di industri 4.0, mesin pabrik

terhubung lewat LAN berbasis Ethernet atau Wi-Fi untuk kontrol real-time, lalu data produksi dikirim ke server pusat melalui WAN.

Meski efektif, integrasi LAN dan WAN menghadapi tantangan. Skalabilitas menjadi isu utama karena jumlah perangkat IoT terus bertambah. Infrastruktur perlu fleksibel dan interoperabel agar mampu menampung jutaan perangkat (Overmars & Venkatraman, 2020). Keamanan juga krusial: data IoT rentan terhadap serangan man-in-the-middle, denial of service, hingga manipulasi routing (Almutairi & Sheldon, 2025). Oleh karena itu, enkripsi dan autentikasi menjadi keharusan. Latensi WAN dapat mengganggu aplikasi kritis real-time, sehingga solusi edge computing banyak digunakan, meski menambah kompleksitas manajemen. Selain itu, faktor biaya—baik instalasi LAN maupun langganan WAN—harus diperhitungkan dalam perencanaan sistem.

Sebagai kesimpulan, LAN dan WAN adalah dua komponen sentral dalam arsitektur IoT. LAN menyediakan koneksi cepat dan andal untuk komunikasi lokal, sedangkan WAN menjamin konektivitas global dan integrasi dengan layanan cloud. Mansour et al. (2023) menekankan peran gateway IoT yang menyatukan keduanya untuk menyalurkan data ke awan. Dengan merancang arsitektur yang memaksimalkan kelebihan LAN dan WAN sekaligus mengatasi kelemahan masing-masing, IoT dapat mendukung aplikasi cerdas berskala global, mulai dari rumah pintar, kota pintar, hingga industri terotomatisasi.

Referensi:

- Almutairi, M., & Sheldon, F. T. (2025). IoT–Cloud Integration Security: A Survey of Challenges, Solutions, and Directions. *Electronics*, 14(7), 1394.
- Dauda, A., Flauzac, O., & Nolot, F. (2024). *A Survey on IoT Application Architectures*. *Sensors*, 24(16), 5320.
- Gerodimos, A., Maglaras, L., Ferrag, M. A., Ayres, N., & Kantzavelou, I. (2023). *IoT: Communication Protocols and Security Threats*. Internet of Things and Cyber-Physical Systems. Keleşoğlu, N., & Sobczak, Ł. (2024). *ZigBeeNet: Decrypted Zigbee IoT Network Traffic Dataset in Smart Home Environment*. *Applied Sciences*, 14(23), 10844.
- Mansour, M., Gamal, A., Ahmed, A. I., Said, L. A., Elbaz, A., Herencsar, N., & Soltan, A. (2023). *Internet of Things: A Comprehensive Overview on Protocols, Architectures, Technologies, Simulation Tools, and Future Directions*. *Energies*, 16(8), 3465.
- Overmars, A., & Venkatraman, S. (2020). *Towards a Secure and Scalable IoT Infrastructure: A Pilot Deployment for a Smart Water Monitoring System*. *Technologies*, 8(4), 50.
- Rayes, A., & Salam, M. A. (Eds.). (2017). *Cloud Technologies and Applications for IoT: Challenges and Solutions*. Springer.
- Al-Fuqaha, M., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). *Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications*. *IEEE Communications Surveys & Tutorials*, 17(4), 2347–2376.
- Li, B., Da Xu, L., & Zhao, S. (2018). *Big Data for Internet of Things: A Survey*. *Sensors*, 18(2), 493.
- Khan, R., & Salah, K. (2018). *IoT Security: Review, Blockchain Solutions, and Open Challenges*. *Future Internet*, 10(3), 33.