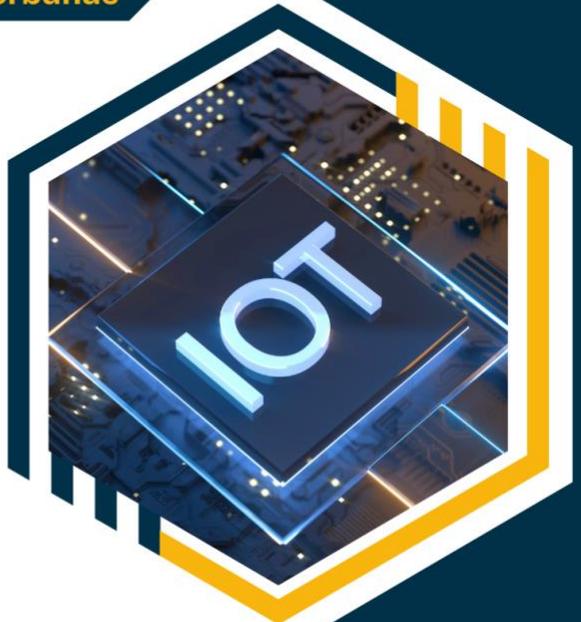


BAB 3

TEKNOLOGI PENDUKUNG INTERNET OF THINGS (IOT)

Program Studi Informatika
Universitas Hayam Wuruk Perbanas



BAB 3

Teknologi Pendukung IoT

A. TUJUAN PEMBELAJARAN

Mahasiswa mampu menjelaskan teknologi pendukung IoT

B. PENDAHULUAN

Pada bab ini akan dijelaskan berbagai teknologi yang secara fungsionalitas dapat mendukung implementasi IoT pada berbagai bidang seperti *cloud computing*, *big data* dan *artificial intelligence*.

C. Cloud Computing

Cloud computing adalah penyediaan sumber daya komputasi komputasi melalui internet, seperti server, penyimpanan, database, jaringan, perangkat lunak, dan alat analitik dapat diakses dan digunakan sesuai kebutuhan. Konsep ini memungkinkan

pengguna untuk menyewa sumber daya komputasi tanpa harus mempunyai dan mengelola infrastruktur fisik sendiri. Layanan *cloud computing* mempunyai pemrosesan dan penyimpanan sesuai permintaan yang dapat digunakan untuk menganalisis data yang dihasilkan oleh objek IoT.

Manfaat *cloud computing* untuk IoT adalah sebagai berikut:

1. **Penyimpanan Skala Besar**

Data yang dihasilkan oleh perangkat IoT bisa dalam jumlah yang sangat besar dan harus disimpan secara efisien. Dengan *cloud computing*, data dapat ditampung dengan kapasitas penyimpanan yang tak terbatas.

2. **Kemampuan Komputasi Yang Tinggi**

Komputasi *cloud computing* memungkinkan analisis data secara real-time dan pembelajaran mesin yang memerlukan daya komputasi tinggi.

3. **Skalabilitas**

Untuk mendukung penambahan perangkat baru atau menangani peningkatan volume data, IoT membutuhkan fleksibilitas. Dengan *cloud computing*, skalabilitas horizontal dapat dicapai dengan mudah.

4. **Keamanan dan Manajemen Data**

Cloud computing memberikan perlindungan ekstra bagi data IoT serta mempermudah pengelolaan data dan integrasi ke berbagai platform.

D. BIG DATA

Big data menggambarkan akuisisi data dengan volume yang besar, kecepatan tinggi, dan keragaman data yang dihasilkan oleh perangkat terkoneksi serta sebuah teknologi dan alat yang digunakan untuk mengelolanya. Big Data untuk IoT adalah konsep di mana data yang dihasilkan oleh berbagai perangkat IoT (*Internet of Things*)

dikumpulkan, disimpan, dianalisis, dan digunakan untuk menghasilkan wawasan yang berguna. Big data juga dapat membantu untuk memahami pola dalam data yang dihasilkan oleh perangkat IoT, mengidentifikasi masalah secara cepat dan memberikan solusi yang lebih efektif, dan juga dapat meningkatkan efisiensi dengan menganalisa data secara langsung. Sebagai contoh dalam perusahaan manufaktur, big data dapat menganalisa data yang dihasilkan oleh perangkat IoT untuk memahami pola kinerja mesin, proses barang jadi dan efisiensi secara menyeluruh. Data yang ada dapat dianalisa secara *real time* sehingga dapat mengidentifikasi secara cepat dan mengambil tindakan yang diperlukan.

E. ARTIFICIAL INTELLIGENCE

Perkembangan teknologi yang cepat memungkinkan berbagai perangkat, seperti perangkat yang dapat dikenakan pada tubuh

manusia, perangkat pada bangunan kota atau perangkat pada transportasi yang terhubung ke internet, untuk saling mengenali dan mengumpulkan serta memproses data. Fenomena ini dikenal sebagai *Internet of Things* (IoT). Selain itu, munculnya perangkat yang dapat belajar dari data dan menyelesaikan tugas dengan cerdas dimungkinkan oleh Artificial Intelligence (AI).

Ketika *Artificial Intelligence* (AI) diterapkan dalam *Internet of Things* (IoT), ini berarti bahwa berbagai perangkat yang terhubung ke internet dapat menganalisis data, membuat keputusan, dan bertindak berdasarkan data tersebut tanpa campur tangan manusia. Akibatnya, terbentuklah perangkat cerdas yang dapat bekerja dengan lebih efektif dan efisien. Konsep kombinasi dua teknologi tersebut sering disebut *AIoT (Artificial Intelligence Internet of Things)*. Kecerdasan dari *AIoT* memungkinkan analisis data yang mengoptimalkan sistem, meningkatkan kinerja, memperluas wawasan bisnis,

dan menyediakan data yang mendukung pengambilan keputusan berdasarkan informasi yang telah dipelajari oleh perangkat tersebut.

Dalam lingkungan ritel yang pintar, sistem kamera dengan kemampuan computer vision dapat menggunakan pengenalan wajah untuk mengidentifikasi pelanggan saat mereka memasuki toko. Sistem ini mengumpulkan data pelanggan, seperti jenis kelamin, preferensi produk, arus lalu lintas, dan lainnya. Kemudian, data tersebut dianalisis secara akurat untuk memprediksi perilaku konsumen dan menggunakan informasi ini untuk membuat keputusan operasional toko, dari pemasaran hingga penempatan produk. Sebagai contoh, jika sistem mendeteksi bahwa mayoritas pelanggan yang masuk adalah generasi milenial, maka sistem akan menampilkan iklan produk atau program spesial yang menarik bagi mereka, sehingga meningkatkan penjualan. Kamera pintar juga dapat mengenali pembeli dan memungkinkan

mereka melewati kasir, seperti yang diterapkan di Amazon Go.

F. SECURITY

Perlindungan perangkat IoT sangat penting karena perangkat tersebut ke internet dan memiliki akses ke berbagai data dan sistem. Penggunaan perangkat IoT telah memberikan manfaat besar dalam banyak aspek kehidupan, akan tetapi hal tersebut juga menimbulkan berbagai risiko keamanan siber yang harus diwaspadai. Beberapa serangan dan potensi risiko terkait perangkat IoT meliputi serangan *brute force*, di mana peretas mencoba menebak kata sandi yang lemah untuk mendapatkan akses ilegal. Selain itu, serangan *Man-in-the-Middle* (MitM) merupakan ancaman di mana peretas mengintersep komunikasi antara perangkat IoT dan server yang memungkinkan mereka mencuri atau mengubah data.

Risiko pencurian data pribadi juga perlu diperhatikan, terutama karena banyak perangkat

IoT mengumpulkan informasi pribadi pengguna yang bisa disalahgunakan oleh peretas. Ada juga risiko serangan DDoS, di mana peretas menggunakan botnet atau komputer zombie untuk melumpuhkan layanan online sehingga menyebabkan gangguan besar pada server. Selain itu, risiko penyusupan sistem perlu dipertimbangkan, di mana peretas bisa mencoba masuk ke jaringan rumah atau bisnis melalui celah pada perangkat IoT yang lemah, membuka peluang untuk serangan lebih lanjut. Oleh karena itu, perhatian serius terhadap keamanan perangkat IoT dan penerapan praktik terbaik untuk melindunginya sangat penting guna menjaga keamanan data dan jaringan.

Untuk melindungi perangkat IoT diperlukan standar keamanan. Beberapa standar telah dikembangkan untuk memastikan keamanan perangkat IoT dan data yang dikumpulkan. Salah satu standar tersebut adalah protokol MQTT (*Message Queuing Telemetry Transport*), sebuah

protokol komunikasi yang dapat dienkrpsi untuk memastikan data yang ditransmisikan antara perangkat dan server tetap aman dari intersepsi pihak yang tidak sah. Selain itu, protokol OAuth (Open Authorization) digunakan untuk mengelola otorisasi akses ke perangkat IoT, memastikan hanya pihak yang sah memiliki izin untuk mengakses data atau mengontrol perangkat.

Selain itu berbagai organisasi dan badan standar telah menyusun panduan dan rekomendasi keamanan khusus untuk perangkat IoT. Misalnya, "IoT Security Foundation" menyediakan pedoman komprehensif untuk mengamankan perangkat IoT, termasuk desain keamanan yang baik, manajemen risiko, dan pengujian perangkat. Sementara itu, "Industrial Internet Consortium" (IIC) menawarkan kerangka kerja keamanan khusus untuk IoT industri yang mencakup prinsip-prinsip seperti identifikasi perangkat, enkripsi, dan deteksi ancaman.

Mematuhi standar keamanan ini menjadi hal yang penting karena tidak hanya untuk melindungi

perangkat IoT dari serangan siber, tetapi juga untuk menjaga data sensitif dan privasi pengguna.

LATIHAN SOAL

1. Jelaskan tentang *Cloud Computing* untuk IoT!
2. Jelaskan tentang *Big Data* untuk IoT!
3. Jelaskan tentang *Artificial Intelligence* untuk IoT!
4. Jelaskan mengapa perangkat IoT perlu dilindungi dari serangan siber!
5. Sebutkan protokol yang menerapkan keamanan!

DAFTAR PUSTAKA

Buyya, R., & Dastjerdi, A. V. (Ed.). (2016). *Internet of Things: Principles and paradigms*. Morgan Kaufmann.

Gomez, C., & Paradells, J. (2010). Wireless home automation networks: A survey of architectures and technologies. *IEEE Communications Magazine*, 48(6), 92–101.
<https://doi.org/10.1109/MCOM.2010.5473869>

Hanes, D., Salgueiro, G., Grossetete, P., Barton, R., & Henry, J. (2017). *IoT fundamentals: Networking technologies, protocols, and use cases for the Internet of things*. Cisco Press.

<https://mysertifikasi.com/>



Kamal, R. (2017). *Internet of things: Architecture and design principles*. Mc Graw Hill India.

Mohamed, K. S. (2019). *The Era of Internet of Things: Towards a Smart World*. Springer International Publishing.
<https://doi.org/10.1007/978-3-030-18133-8>