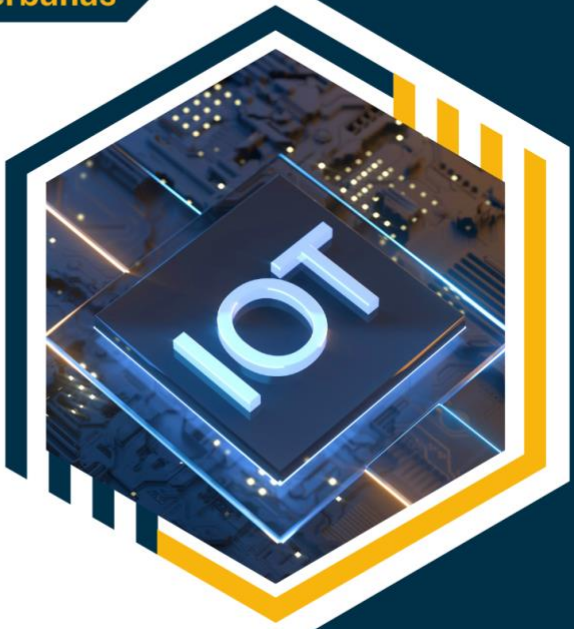
BAB 8

APPLICATION PROGRAMMING INTERFACE (API)

INTERNET OF THINGS (IOT)

Program Studi Informatika
Universitas Hayam Wuruk Perbanas



BAB 8
API IoT

A. TUJUAN PEMBELAJARAN

Mahasiswa mampu mendemonstrasikan API IoT.

B. PENDAHULUAN

Pada bab ini akan dijelaskan fungsi dari API pada perangkat IoT serta komunikasi dan mekanisme keamanan pada API.

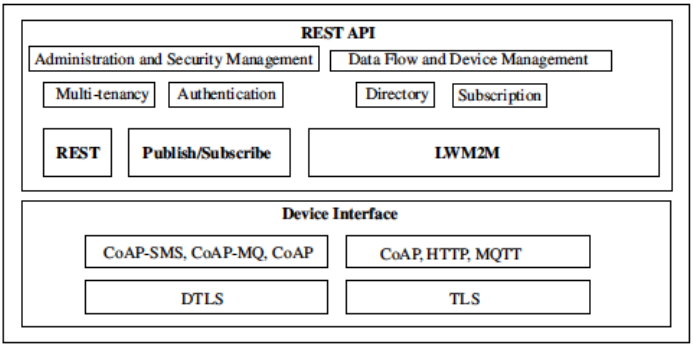
C. API

API *(Application Programming Interface)* IoT adalah sebuah antarmuka yang memungkinkan perangkat IoT untuk berkomunikasi dengan aplikasi lain, baik itu aplikasi web, aplikasi mobile, atau layanan cloud. Dengan API, memungkinkan integrasi antara perangkat yang berbeda untuk berbagi data san berinteraksi satu sama lain secara efisen dan aman. Sangat penting untuk menerapkan

manajemen API yang terukur dan aman karena API menghubungkan hal penting ke sistem IoT. API bisa berupa layanan eksternal yang memerlukan kunci akses untuk digunakan, atau bisa juga sepenuhnya gratis dan tersedia untuk umum tanpa perlu pendaftaran ke penyedianya.

Integrasi website dengan IoT bertujuan untuk memanfaatkan data yang dihasilkan oleh perangkat IoT secara jarak jauh dan *real time* melalui antarmuka website. Integrasi tersebut memungkinkan pengguna mengakses informasi secara langsung dan *real time.* Sebagai contoh data suhu ruang yang dapat ditampilkan secara instan. Selain itu dengan mengintegrasikan website dengan perangkat IoT, data dapat diotomatisasi dan disinkronkan secara lebih efisien. Sehingga akan mengurangi kerja manual, meningkatkan produktivitas, dan memastikan keakuratan data. Pengelolaan data yang lebih efektif juga mendukung analisis yang lebih mendalam, memungkinkan

pengambilan keputusan yang lebih cerdas. Beberapa contoh platform IoT yang menyediakan API seperti Google Cloud IoT, AWS IoT, Microsoft Azure IoT. Antarmuka konektivitas terdiri dari komunikasi API, antarmuka perangkat dan pemrosesan unit.



Gambar 8.1 API dan Antarmuka Komponen Perangkat

D. FUNGSI API

Penggunaan API menjadi fondasi utama dalam menghubungkan website dengan perangkat IoT. API berperan sebagai jembatan atau perantara yang memungkinkan dua entitas tersebut. API menjadi titik akses yang memungkinkan website untuk mengambil, mengirim dan memproses data dari

perangkat IoT dan sebaliknya. Sehingga pemilihan protokol pertukaran pesan harus disesuaikan dengan kebutuhan. API IoT mempunyai beberapa fungsi sebagai berikut:

1. **Komunikasi Data**

   API IoT memungkinkan perangkat untuk mengirim dan menerima data. Sebagai contoh, sensor kelembaban dapat mengirim data sensor ke server melalui API, dan server dapat mengirim perintah kembali ke perangkat untuk mengambil tindakan tertentu.

2. **Manajemen Perangkat**

   API IoT memungkinkan pengelolaan perangkat seperti menambah, menghapus, atau mengupdate konfigurasi perangkat yang terhubung dalam jaringan IoT.

3. **Otentikasi dan Keamanan**

   API IoT dapat dilengkapi dengan mekanisme otentikasi dan enkripsi untuk memastikan bahwa

data yang dikirimkan dan diterima aman dari akses yang tidak sah.

E. MONITORING DENGAN API

Pemantauan perangkat melalui API dapat membantu di banyak domain. Sebagai contoh untuk pemantauan status sensor, kinerja peralatan, pelaporan penggunaan daya. Aplikasi *real time* dapat memanfaatkan fitur REST API Telemetry untuk melaporakan status sistem IoT. REST API Telemetry adalah *Application Programing Interface (API)* yang memungkinkan pengguna untuk mengakses data sensor secara *real time* dari perangkat IoT menggunakan protokol HTTP. Sehingga pengguna dapat mengambil data sensor yang dikirim oleh perangkat IoT ke platform atau layanan cloud. Data tersebut kemudian dapat digunakan untuk analisis, pemantauan, otomatisasi dan integrasi dengan aplikasi pihak ketiga.

F. KEAMANAN API

Keamanan API mengacu pada pratik dan prosedur untuk melindungi API dari serangan eksternal seperti serangan bot dan penyalahgunaan wewenang. Keamanan pada API awalnya berfokus pada komunikasi antar proses dalam satu sistem. Sehingga keamanan tidak menjadi perhatian karena komunikasi hanya terbatas pada satu mesin. Namun dengan munculnya *Internet of Things,* API diperluas untuk memungkinkan komunikasi yang lancar dan perutean panggilan antar aplikasi dan di seluruh lingkungan DevOps. APU modern yang mempunyai kualitas tinggi saat ini mampu melakukan fungsi seperti transfer status representasi (REST)dan protokol akses objek sederhana (SOAP).

Jika API tidak diamankan dengan benar, hal ini dapat memungkinkan penjahat siber untuk melakukan hal-hal yang tidak diinginkan. Beberapa ancaman yang dapat terjadi meliputi.

- Serangan berbasis autentikasi yaitu ketika peretas mencoba menebak atau mencuri kata sandi pengguna untuk mendapatkan akses ke server API.
- Serangan man-in-the-middle yaotu ketika penjahat mencegat permintaan atau respon API yang dikirim dari pengirim ke penerima untuk mencuri atau momodifikasi data.
- Serangan injeksi kode dimana peretas mengirimkan skri berbahaya melalui permintaan API dengan mengeksploitasi kelememahan pada penerjemah API yang membaca dan menerjemahkan data. Hal ini dilakukan untuk menyisipkan informasi palsu, menghapus data atau menggaggu fungsionalitas aplikasi.
- Serangan *Denial of Service* (DoS) yaitu serangan ini mengirimkan sejumlah permintaan API yang membuat server melambat. Serangan DoS dapat datang dari beberapa penyerang secara bersamaan yang

disebut sebagai *Distributed denial-of-service* (DdoS).

G. KEAMANAN IOT

Praktik yang dapat dilakukan untuk mengamankan sistem IoT adalah sebagai berikut:

- Perbarui perangkat IoT dengan versi perangkat lunak *(firmware)* terbaru, karena dengan versi terbaru terdapat perbaikan keamanan yang penting.
- Gunakan kata sandi yang kuat untuk melindungi perangkat dan akun terkait. Hindari penggunaan kata sandi sederhana atau yang mudah ditebak.
- Melakukan enkripsi data yang dikirim antara perangkat IoT dan server terenkripsi. Gunakan protokol yang aman, seperti HTTPS atau MQTT dengan SSL/TLS.

- Gunakan protokol otorisasi seperti Oauth untuk mengatur akses pengguna ke perangkat IoT dan data mereka.
- Pastikan firewall dan perangkat keamanan jaringan lainnya dikonfigurasi dengan baik untuk mengawasi dan melindungi perangkat IoT.
- Gunakan alat pemantauan dan deteksi ancaman untuk melacak aktivitas mencurigakan pada perangkat IoT. Atur notifikasi peringatan untuk pemberitahuan segera apabila ada aktivitas yang mencurigakan.

H. LATIHAN SOAL

1. Jelaskan tentang API!
2. Jelaskan fungsi API!
3. Apa yang dimaksud dengan REST API Telemetry!
4. Jelaskan fungsi API sebagai monitoring perangkat IoT!
5. Sebutkan dan jelaskan serangan-serangan pada API!

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.

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