

DASAR-DASAR DAN APLIKASI INTERNET OF THINGS (IOT)

TIM PENULIS :

Wahyuddin S
Dwi Feriyanto
Dwi Sasmita Aji Pambudi
Muhammad Nuzan Rizki
Ali Impron
Tasrif Hasanuddin
Yendi Putra
Frabowo Praselia
Cahyo Wibowo
Fitri Duspasari
Muh. Agus



DASAR-DASAR DAN APLIKASI *INTERNET OF THINGS (IoT)*

**Wahyuddin S
Dwi Feriyanto
Dwi Sasmita Aji Pambudi
Muhammad Nuzan Rizki
Ali Impron
Tasrif Hasanuddin
Yendi Putra
Frabowo Prasetya
Cahyo Wibowo
Fitri Puspasari
Muh. Agus**



GETPRESS INDONESIA

DASAR-DASAR DAN APLIKASI *INTERNET OF THINGS* (IoT)

Penulis :

Wahyuddin S
Dwi Feriyanto
Dwi Sasmita Aji Pambudi
Muhammad Nuzan Rizki
Ali Impron
Tasrif Hasanuddin
Yendi Putra
Frabowo Prasetya
Cahyo Wibowo
Fitri Puspasari
Muh. Agus

ISBN : 978-623-125-732-1

Editor : Hendra Nusa Putra, S.Kom., M.kom.

Desain Sampul dan Tata Letak : Atyka Trianisa, S. Pd.

Penerbit: CVGETPRESS INDONESIA

Anggota IKAPI No. 033/SBA/2022

Redaksi:

Jl. Palarik RT 01 RW 06, Kelurahan Air Pacah
Kecamatan Koto Tengah, Padang, Sumatera Barat

website: www.getpress.co.id
email: adm.getpress@gmail.com

Cetakan Pertama, Maret 2025

Hak cipta dilindungi undang-undang
Dilarang memperbanyak karya tulis ini dalam bentuk
dan dengan cara apapun tanpa izin tertulis dari penerbit.

KATA PENGANTAR

Dengan mengucapkan puji syukur kehadiran Allah SWT, atas limpahan rahmat dan hidayahNya, maka Penulisan Buku dengan judul *Dasar-Dasar dan Aplikasi Internet of Things (IoT)* dapat diselesaikan dengan kerjasama tim penulis. Dasar-Dasar dan Aplikasi *Internet of Things* merupakan buku berisikan bahasan mengenai pengantar IoT, arsitektur dan desain IoT, “things” pada IoT, prinsip koneksi pada IoT, IP sebagai lapisan jaringan pada IoT, protokol aplikasi pada IoT, keamanan IoT, implementasi IoT pada industri manufaktur, implementasi IoT pada bidang minyak dan gas, implementasi IoT pada bidang transportasi dan healthcare, dan implementasi IoT pada bidang pertanian dan lingkungan.

Buku ini masih banyak kekurangan dalam penyusunannya. Oleh karena itu, kami sangat mengharapkan kritik dan saran demi perbaikan dan kesempurnaan buku ini selanjutnya. Kami mengucapkan terima kasih kepada berbagai pihak yang telah membantu dalam proses penyelesaian Buku ini. Semoga Buku ini dapat menjadi sumber referensi dan literatur yang mudah dipahami.

Padang, Maret 2025
Penulis

DAFTAR ISI

KATA PENGANTAR.....	i
DAFTAR ISI	ii
DAFTAR GAMBAR.....	v
DAFTAR TABEL	vii
BAB 1 PENGANTAR IoT	1
1.1 Pendahuluan.....	1
1.2 Sejarah dan Perkembangan IoT	2
1.3 Komponen Utama IoT.....	5
1.4 Manfaat dan Potensi IoT.....	8
1.5 Tantangan dan Isu.....	10
DAFTAR PUSTAKA	11
BAB 2 ARSITEKTUR DAN DESAIN IoT	12
2.1 Pendahuluan.....	12
2.2 Arsitektur IoT.....	14
DAFTAR PUSTAKA	29
BAB 3 “THINGS” PADA IoT	30
3.1 Pengertian "Things" dalam IoT.....	30
3.2 Peran dan Fungsi utama “Things” dalam IoT.....	32
3.3 Optimalisasi Kinerja “Things” dalam Sistem IoT	35
3.4 Klasifikasi “Things” dalam Sistem IoT.....	38
3.5 Sensor dan Aktuator sebagai Bagian dari IoT	45
3.6 Unit Pemrosesan Data dalam IoT	53
DAFTAR PUSTAKA	58
BAB 4 PRINSIP KONEKSI PADA IoT	61
4.1 Pendahuluan.....	61
4.2 Dasar-Dasar Koneksi.....	62
4.3 Protokol Koneksi IoT	64
4.4 Teknologi Koneksi IoT.....	66
DAFTAR PUSTAKA	72
BAB 5 IP SEBAGAI LAPISAN JARINGAN PADA IoT	74
5.1 Pendahuluan.....	74
5.2 Konsep Dasar Internet Protocol (IP) dalam IoT	76
5.3 Perbedaan IPv4 dan IPv6 pada IoT.....	77
5.4 Pengelolaan Alamat IP dalam Jaringan IoT	80
5.5 Protokol Pendukung untuk IP dalam IoT	83
5.6 Keamanan IP pada IoT	86

5.7 Pemanfaatan IP Multicast dalam IoT	88
5.8 IP dan Pengoptimalan Jaringan pada IoT	90
5.9 Kesimpulan	92
DAFTAR PUSTAKA.....	94
BAB 6 PROTOKOL APLIKASI PADA IoT	96
6.1 Pendahuluan.....	96
6.2 Protokol MQTT (<i>Message Queuing Telemetry Transport</i>).....	98
6.3 <i>Constrained Application Protocol</i> (CoAP).....	110
6.4 Protokol HTTP/HTTPS (<i>HyperText Transfer Protocol</i>)	116
DAFTAR PUSTAKA.....	119
BAB 7 KEAMANAN IoT	120
7.1 Pendahuluan.....	120
7.2 Pentingnya Keamanan Pada IoT	122
7.3 Regulasi dan Standar Keamanan IoT	124
7.4 Kasus-kasus Serangan Pada IOT	128
7.5 Jenis-jenis Serangan Pada IoT	130
7.6 Penanganan Dan Strategi Keamanan IOT	132
7.7 Praktik Pengamanan IoT	150
DAFTAR PUSTAKA.....	163
BAB 8 IMPLEMENTASI IoT PADA INDUSTRI MANUFAKTUR.....	166
8.1 Implementasi IoT pada Industri.....	166
8.2 Siklus Manufaktur: Langkah-langkah dalam Proses Produksi	168
8.3 Implementasi <i>Internet of Things</i> (IoT) dalam Pengelolaan Proses.....	173
8.4 Pemanfaatan Mesin: Meningkatkan Produktivitas dan Efisiensi Operasional	175
8.5 Pemeliharaan Terprediksi: Meningkatkan Efisiensi dan Ketersediaan Mesin.....	176
DAFTAR PUSTAKA.....	179
BAB 9 IMPLEMENTASI IOT PADA BIDANG MINYAK DAN GAS	180
9.1 Pendahuluan.....	180
9.2 Pengertian Migas	182
9.3 Proses Migas.....	184
9.4 Klasifikasi Produk Industri Migas.....	184
9.5 IoT Untuk Industri Migas	185
9.6 Penutup	206
DAFTAR PUSTAKA.....	207

BAB 10 IMPLEMENTASI IOT PADA BIDANG TRANSPORTASI	
DAN HEALTHCARE	209
10.1 Pendahuluan	209
10.2 Penerapan IoT dalam Transportasi Cerdas	210
10.3 IoT dalam <i>Healthcare</i>	214
DAFTAR PUSTAKA	221
BAB 11 IMPLEMENTASI IoT PADA BIDANG PERTANIAN DAN	
LINGKUNGAN	222
11.1 Pendahuluan	222
11.2 Teknologi IoT dalam Pertanian.....	225
11.3 Teknologi IoT dalam Lingkungan	229
11.4 Keuntungan dan Tantangan Implementasi IoT.....	233
11.5 Studi Kasus dan Masa Depan	234
11.6 Praktikum IoT pada Pertanian dan Lingkungan.....	234
11.7 Kesimpulan.....	239
DAFTAR PUSTAKA	240
BIODATA PENULIS	244

DAFTAR GAMBAR

Gambar 1. 1 <i>Internet of Things</i>	2
Gambar 2. 1 Lapisan Arsitektur IoT.....	14
Gambar 2. 2 <i>Perception Layer</i> (Lapisan Persepsi)	15
Gambar 2. 3 Jenis-Jenis Sensor.....	16
Gambar 2. 4 Jenis Aktuator.....	17
Gambar 2. 5 Kamera CCTV/Thermal.....	17
Gambar 2. 6 Robot.....	18
Gambar 2. 7 Meter Pengukuran Tegangan Listrik.....	19
Gambar 2. 8 Lapisan <i>Network</i> (Lapisan Jaringan)	20
Gambar 2. 9 Lapisan <i>Processing</i> (Lapisan Pemrosesan).....	24
Gambar 2. 10 Lapisan <i>Application</i> (Lapisan Aplikasi)	27
Gambar 3. 1 Karakteristik <i>Things</i> dalam IoT	31
Gambar 3. 2 Klasifikasi Objek " <i>Things</i> "	40
Gambar 3. 3 Karakteristik Objek Cerdas (<i>Smart Objects</i>)	42
Gambar 4. 1 Kemampuan Konektifitas Antar Perangkat dalam Ekosistem IoT	63
Gambar 4. 2 Ilustrasi Penggunaan Teknologi Wi-fi dalam Komunikasi Antar Perangkat IoT	67
Gambar 5. 1 Grafik Kehabisan Alamat IPv4	77
Gambar 5. 2 Cara Kerja DNS	82
Gambar 7. 1 Ilustrasi IoT	121
Gambar 7. 2 GDPR	125
Gambar 8. 1 Enkripsi Simetris.....	135
Gambar 7. 3 Algoritma AES	137
Gambar 7. 4 Enkripsi Asimetris.....	140
Gambar 9. 1 Ilustrasi Data Transfer.....	181
Gambar 9. 2 Ilustrasi Aplikasi IoT Migas	181
Gambar 9. 3 Sumur Minyak Sebagai Sumber Migas.....	182
Gambar 9. 4 <i>Production Process Overview</i>	183
Gambar 9. 5 Diagram Alir Proses Minyak Bumi Menjadi Produk Siap Pakai	184
Gambar 9. 6 Diagram Proses IoT Pemantauan Sumur Migas	188
Gambar 9. 7 Tampilan IoT <i>Dashboard</i> Pemantauan Sumur Migas.....	188
Gambar 9. 8 Arsitektur Sistem IoT Pemantau Sumur Migas.....	189
Gambar 9. 9 Piktorial Informasi dari Sebuah Sumur Minyak oleh IoT...	190
Gambar 9. 10 Aktivitas Ruang Control dan Monitoring pada Sumur Minyak.....	190
Gambar 9. 11 <i>Dashboard</i> Pemantauan Sumur	191

Gambar 9. 12 Visualisasi Menggunakan <i>Thermal Camera</i> untuk Deteksi awal.....	194
Gambar 9. 13 Camera Pemantau di Area Berbahaya	195
Gambar 9. 14 Pengukuran Ketinggian Permukaan Terhadap Tangki Minyak.....	195
Gambar 9. 15 Recording Level Transmitter dengan Output RS485	196
Gambar 9. 16 Sensor Suara (<i>Sound Sensor</i>)	197
Gambar 9. 17 <i>Acoustic Sensor</i>	197
Gambar 9. 18 Gas Detector Portable Berfungsi sebagai Pengaman Pekerja yang Dapat Dikirimkan Melalui <i>Cloud</i>	198
Gambar 9. 19 <i>Leak Detector Robot</i>	199
Gambar 9. 20 <i>Wheatstone Bridge</i>	200
Gambar 9. 21 Aplikasi Sensor Akustik pada Instalasi Migas.....	202
Gambar 9. 22 Aplikasi Sensor Seismik Bawah Laut.....	203
Gambar 9. 23 <i>Computerized Gas Monitoring System (CGMS)</i>	204
Gambar 9. 24 <i>Aplikasi IoT-Microcontroller</i> pada CGMS.....	205
Gambar 10. 1 Simulasi Sistem Pengendalian Lalu Lintas Berbasis IoT	211
Gambar 10. 2 Sistem Navigasi dan Pemantauan Penerbangan Berbasis IoT	212
Gambar 10. 3 Teknologi IoT dalam Sistem Pemantauan Armada	213
Gambar 10. 4 Teknologi IoT dalam Sistem Sistem Parkir Pintar	214
Gambar 10. 5 <i>Smartwatch</i>	215
Gambar 10. 6 ECG Monitor	216
Gambar 10. 7 Oximeter	217
Gambar 10. 8 Glucometer	217
Gambar 10. 9 Layanan Telemedicine	218
Gambar 10. 10 Layanan <i>Telemedicine</i>	219

DAFTAR TABEL

Tabel 6. 1 Perbandingan QOS Level pada MQTT.....	104
Tabel 7. 1 Kasus-kasus Serangan Pada IoT.....	128
Tabel 7. 2 Keunggulan dan Kelemahan Enkripsi Simetris	138
Tabel 7. 3 Keunggulan dan Kelemahan Enkripsi Asimetris.....	141
Tabel 7. 4 Perbedaan IDS dan IPS	155
Tabel 7. 5 Alat yang Digunakan dalam Simulasi <i>Penetration Testing</i> IoT	160
Tabel 9. 1. Parameter yang Dapat Diukur dan Dikirim dengan IoT	187

BAB 1

PENGANTAR IoT

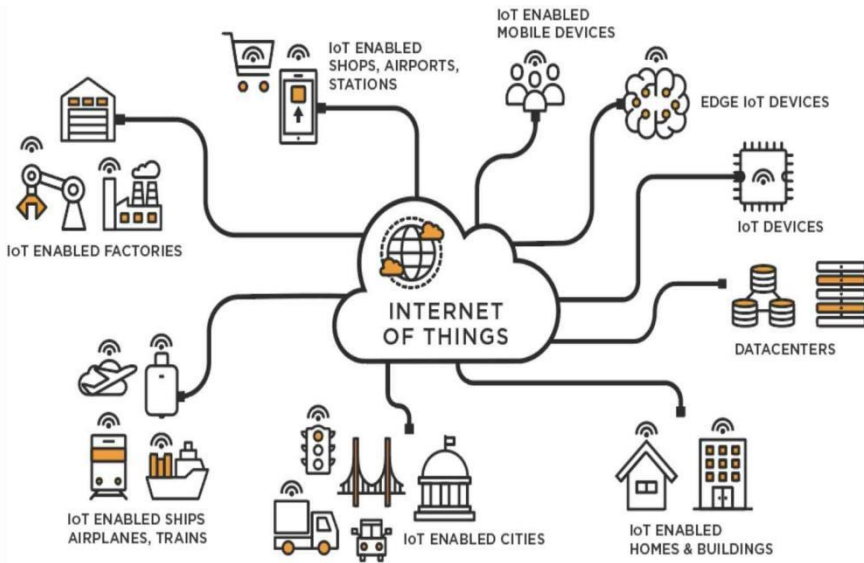
Oleh Wahyuddin S

1.1 Pendahuluan

Dalam era digital yang terus berkembang, konsep *Internet of Things* (IoT) telah menjadi salah satu inovasi teknologi paling signifikan dan transformatif. IoT merujuk pada jaringan perangkat fisik yang saling terhubung melalui internet, memungkinkan untuk mengumpulkan dan menganalisis data dengan tujuan meningkatkan efisiensi, keamanan, dan kenyamanan dalam berbagai aspek kehidupan manusia (Wibowo et al., 2023).

Sejak ditemukannya internet, komunikasi telah berubah secara drastis. IoT memperluas kemampuan internet untuk mencakup perangkat fisik, memungkinkan interaksi yang lebih cerdas antara berbagai perangkat dan sistem. Ide dasar IoT adalah untuk mengintegrasikan perangkat fisik dengan teknologi digital, menciptakan ekosistem yang saling terhubung dan berfungsi secara otonom.

IoT dapat didefinisikan sebagai jaringan dari perangkat fisik yang dilengkapi dengan sensor, perangkat lunak, dan teknologi lainnya yang memungkinkan untuk terhubung dan bertukar data dengan perangkat lain melalui internet. Perangkat-perangkat ini dapat berupa apa saja, mulai mesin industri, kendaraan, dan perangkat medis (Ramadhan et al., 2023).



Gambar 1. 1 *Internet of Things*
 (<https://www.visiniaga.com/id/blog/our-blog-1/internet-of-things-54>)

1.2 Sejarah dan Perkembangan IoT

Internet of Things (IoT) telah berkembang dari konsep teoretis menjadi salah satu inovasi teknologi paling signifikan di dunia modern (Muttaqin, Yuswardi, Parewe, et al., 2023). Berikut adalah gambaran sejarah dan perkembangan IoT dari masa ke masa:

Awal Mula Konsep

- 1960-an hingga 1980-an: Konsep dasar mengenai perangkat yang terhubung muncul seiring dengan berkembangnya teknologi komputer dan komunikasi. Namun, pada masa ini, koneksi antara perangkat terbatas pada lingkungan tertutup seperti jaringan perusahaan.
- 1982: Mesin penjual Coca-Cola di Carnegie Mellon University, Pittsburgh, menjadi perangkat pertama yang terhubung ke internet, mengirimkan laporan stok dan suhu

minuman. Ini dianggap sebagai prototipe awal dari perangkat IoT.

Tahun 1990-an: Awal dari IoT

- 1991: Mark Weiser, seorang peneliti di Xerox PARC, memperkenalkan konsep "komputasi ubiquitous," yang menggambarkan visi perangkat yang saling terhubung dan dapat berkomunikasi secara seamless.
- 1999: Istilah "Internet of Things" pertama kali diperkenalkan oleh Kevin Ashton, seorang peneliti di Procter & Gamble, dalam konteks manajemen rantai pasokan. Ashton melihat potensi besar dalam menghubungkan perangkat fisik ke internet untuk meningkatkan efisiensi dan transparansi.

Tahun 2000-an: Penerapan Awal dan Penelitian

- 2000-an Awal: Penelitian dan pengembangan IoT mulai berkembang di berbagai universitas dan perusahaan teknologi. Fokusnya adalah pada sensor, RFID (*Radio Frequency Identification*), dan teknologi komunikasi nirkabel.
- 2008-2009: Cisco memperkirakan bahwa jumlah perangkat yang terhubung ke internet telah melampaui jumlah populasi manusia di bumi, menandai awal dari era IoT (Wahyuddin, Heryana, et al., 2023).

Tahun 2010-an: Pertumbuhan dan Adopsi

- 2010: Komunitas teknologi mulai mengakui potensi besar dari IoT, dengan berbagai konferensi dan publikasi ilmiah yang membahas topik ini.
- 2011: McKinsey Global Institute menerbitkan laporan yang memperkirakan dampak ekonomi besar dari IoT, menggarisbawahi potensi transformasi di berbagai industri.
- 2013: IoT menjadi fokus utama dalam Consumer Electronics Show (CES) di Las Vegas, menunjukkan berbagai produk

konsumen yang terhubung seperti thermostat pintar, alat rumah tangga, dan perangkat kesehatan.

- 2014: Google mengakuisisi Nest Labs, sebuah perusahaan yang terkenal dengan thermostat pintarnya, menandai minat besar dari perusahaan teknologi besar dalam IoT.
- 2016: Serangan DDoS besar-besaran menggunakan perangkat IoT yang tidak aman menunjukkan kerentanan dan tantangan keamanan yang signifikan dalam ekosistem IoT.

Tahun 2020-an: Konsolidasi dan Pengembangan Lanjut

- 2020: Pandemi COVID-19 mendorong adopsi teknologi IoT di sektor kesehatan dan logistik, dengan meningkatnya permintaan akan pemantauan jarak jauh dan manajemen rantai pasokan yang efisien.
- 2021: IoT terus berkembang dengan penerapan yang lebih luas dalam smart cities, kendaraan otonom, dan industri 4.0. Teknologi 5G mulai diimplementasikan, memberikan konektivitas yang lebih cepat dan andal untuk perangkat IoT.
- 2022: Jumlah perangkat IoT diperkirakan mencapai lebih dari 20 miliar, mencakup berbagai sektor termasuk kesehatan, pertanian, manufaktur, dan rumah pintar (Muttaqin, Yuswardi, Warni, et al., 2023).

Tren Masa Depan

- Konektivitas 5G: Implementasi teknologi 5G diharapkan akan mempercepat adopsi IoT dengan memberikan kecepatan data yang lebih tinggi, latensi yang lebih rendah, dan kapasitas yang lebih besar.
- Kecerdasan Buatan (AI): Integrasi AI dengan IoT akan meningkatkan kemampuan analitik dan otomatisasi, memungkinkan perangkat untuk membuat keputusan yang lebih cerdas.

- Keamanan dan Privasi: Fokus pada pengembangan standar keamanan dan privasi yang lebih baik untuk melindungi data dan perangkat dari ancaman siber.
- *Edge Computing*: Mengurangi latensi dengan memproses data lebih dekat ke sumbernya, memungkinkan respon yang lebih cepat dan efisien.

1.3 Komponen Utama IoT

Internet of Things (IoT) terdiri dari berbagai komponen yang bekerja bersama untuk mengumpulkan, mengirim, dan menganalisis data guna menghasilkan wawasan yang berguna dan otomatisasi proses (Haris et al., 2023). Berikut adalah penjelasan tentang komponen utama IoT:

Perangkat Fisik (*Things*)

- Sensor
Sensor digunakan untuk mendeteksi dan mengukur kondisi lingkungan atau parameter tertentu, seperti suhu, kelembaban, cahaya, gerakan, tekanan, dan lainnya. Sensor ini mengumpulkan data mentah yang kemudian dikirim untuk diproses.
- Aktuator
Aktuator adalah perangkat yang mengambil tindakan berdasarkan instruksi yang diterima dari sistem kontrol IoT. Contohnya termasuk motor listrik yang menggerakkan mesin, katup yang membuka atau menutup aliran cairan, atau pemanas yang mengatur suhu.
- Perangkat Pintar
Termasuk alat rumah tangga pintar, perangkat medis, kendaraan, dan berbagai jenis perangkat elektronik lainnya yang dilengkapi dengan sensor dan aktuator serta kemampuan komunikasi.

Konektivitas

- Protokol dan Teknologi Jaringan
IoT menggunakan berbagai protokol komunikasi dan teknologi jaringan untuk menghubungkan perangkat ke internet. Beberapa di antaranya adalah:
- Wi-Fi
Digunakan untuk konektivitas nirkabel di lingkungan dengan jaringan internet yang tersedia.
- Bluetooth
Cocok untuk komunikasi jarak pendek antara perangkat.
- Zigbee
Digunakan untuk aplikasi IoT yang membutuhkan daya rendah dan jaringan mesh.
- NFC (*Near Field Communication*)
Digunakan untuk komunikasi jarak sangat pendek, sering digunakan untuk pembayaran dan akses kontrol.
- LPWAN (*Low Power Wide Area Network*)
Termasuk teknologi seperti LoRaWAN dan Sigfox yang memungkinkan komunikasi jarak jauh dengan konsumsi daya rendah.
- 5G
Teknologi seluler generasi terbaru yang menawarkan kecepatan data tinggi, latensi rendah, dan kapasitas yang lebih besar (Wahyuddin, Rismayani, et al., 2023).

Edge Computing

Pemrosesan di Edge: *Edge computing* mengacu pada pemrosesan data yang dilakukan di dekat sumber data itu sendiri, seperti pada perangkat IoT atau di edge gateway. Ini mengurangi latensi dan beban pada jaringan dengan memproses data secara lokal sebelum mengirimkannya ke cloud atau pusat data.

Platform IoT

- **Manajemen Perangkat**
Platform IoT menyediakan alat untuk mengelola perangkat yang terhubung, termasuk konfigurasi, pemantauan status, pembaruan perangkat lunak, dan diagnostik.
- **Pengumpulan dan Penyimpanan Data**
Platform ini mengumpulkan data dari perangkat IoT dan menyimpannya untuk analisis lebih lanjut. Data ini dapat disimpan di cloud atau infrastruktur lokal.
- **Analitik dan Pemrosesan Data**
Platform IoT menganalisis data yang dikumpulkan untuk menghasilkan wawasan yang berguna, seperti pola penggunaan, anomali, atau prediksi berbasis data.
- **Keamanan dan Privasi**
Platform IoT harus memastikan keamanan data dan perangkat melalui enkripsi, otentikasi, dan kontrol akses.

Aplikasi dan Layanan IoT

- **Aplikasi Konsumen**
Termasuk aplikasi rumah pintar yang memungkinkan pengguna untuk mengontrol dan memantau perangkat rumah tangga, aplikasi kesehatan untuk pemantauan kesehatan pribadi, dan aplikasi kendaraan untuk manajemen kendaraan yang lebih baik.
- **Aplikasi Industri**
Termasuk aplikasi untuk manajemen pabrik, pemantauan kondisi mesin, manajemen rantai pasokan, dan otomatisasi proses industri.
- **Aplikasi Komersial**
Termasuk aplikasi untuk manajemen gedung pintar, pemantauan lingkungan kerja, dan sistem keamanan komersial (Nuraini et al., 2023).

Integrasi Kecerdasan Buatan (AI)

- *Machine Learning*
Algoritma machine learning digunakan untuk menganalisis data IoT dan membuat prediksi atau rekomendasi berdasarkan pola yang terdeteksi.
- *Computer Vision*
Digunakan dalam aplikasi IoT yang memerlukan pengenalan objek atau analisis gambar, seperti sistem keamanan atau kendaraan otonom.
- *Natural Language Processing (NLP)*
Digunakan dalam asisten virtual dan sistem kontrol suara untuk memahami dan menanggapi perintah suara (Dawis et al., 2022).

1.4 Manfaat dan Potensi IoT

IoT memiliki potensi untuk membawa perubahan besar dalam berbagai bidang, seperti:

Transformasi Industri

- **Industri 4.0**
Integrasi IoT dalam manufaktur dan produksi dikenal sebagai Industri 4.0, yang menggabungkan otomatisasi, data real-time, dan analisis untuk meningkatkan efisiensi dan fleksibilitas.
- **Pertanian Pintar**
IoT memungkinkan pemantauan kondisi tanah, cuaca, dan tanaman, membantu petani dalam meningkatkan hasil panen dan mengelola sumber daya dengan lebih efisien (Wahyuddin, Istiono, et al., 2023).

Pengembangan Smart Cities

- **Manajemen Lalu Lintas**
Sensor IoT dan sistem analitik dapat mengelola lalu lintas secara real-time, mengurangi kemacetan dan meningkatkan keselamatan.
- **Pengelolaan Limbah**
IoT dapat digunakan untuk memantau dan mengelola sistem pengelolaan limbah, meningkatkan efisiensi dan keberlanjutan.

Inovasi dalam Kesehatan

- **Pemantauan Kesehatan Jarak Jauh**
Perangkat medis yang terhubung memungkinkan dokter untuk memantau kondisi pasien dari jarak jauh, memberikan perawatan yang lebih responsif dan personal.
- *Telemedicine*
Integrasi IoT dengan layanan *telemedicine* memungkinkan konsultasi medis jarak jauh, mengurangi kebutuhan kunjungan fisik ke fasilitas kesehatan.

Transportasi dan Logistik

- **Kendaraan Otonom**
IoT memainkan peran penting dalam pengembangan kendaraan otonom, memungkinkan komunikasi antara kendaraan dan infrastruktur jalan.
- **Manajemen Rantai Pasokan**
Sensor IoT dapat memantau kondisi produk selama transportasi, memastikan kualitas dan keamanan, serta mengoptimalkan rantai pasokan.

Lingkungan dan Keberlanjutan

- **Pemantauan Lingkungan**
IoT dapat digunakan untuk memantau kondisi lingkungan seperti kualitas udara, air, dan tanah, membantu dalam menjaga keberlanjutan dan mengatasi perubahan iklim.

- **Energi Terbarukan**
Sistem manajemen energi berbasis IoT dapat mengintegrasikan dan mengelola sumber energi terbarukan dengan lebih efisien.

1.5 Tantangan dan Isu

Meskipun memiliki banyak manfaat, IoT juga menghadapi beberapa tantangan, antara lain:

- **Keamanan dan Privasi**
Melindungi data dan sistem dari serangan siber.
- **Interoperabilitas**
Memastikan perangkat dari berbagai produsen dapat bekerja sama dengan baik.
- **Kompleksitas Infrastruktur**
Mengelola jaringan yang besar dan kompleks dari perangkat yang terhubung.
- **Regulasi**
Mematuhi aturan dan regulasi yang berlaku di berbagai wilayah.

DAFTAR PUSTAKA

- Dawis, A. M., Himawan, I. S., Meidelfi, D., Ikhrum, F., Intan, I., Harun, R., ... Purnomo, R. (2022). *Artificial Intelligence: Konsep Dasar Dan Kajian Praktis*. TOHAR MEDIA.
- Haris, M. S., Nurlaila, Q., Ratnadewi, R., Friadi, J., Hendrawan, S. A., Meidelfi, D., ... Dewi, A. R. S. (2023). *PENGANTAR DATA SCIENCE*. Penerbit Widina.
- Muttaqin, M., Yuswardi, Y., Parewe, A. M. A. K., Ashari, I. F., Munsarif, M., Wahyuddin, S., ... Gustiana, Z. (2023). *Pengantar Sistem Cerdas*. Yayasan Kita Menulis.
- Muttaqin, M., Yuswardi, Y., Warni, E., Wahyuddin, S., Bagaskara, R., Ambarwari, A., ... Sinambela, M. (2023). *Konsep Dasar Kecerdasan Buatan*. Yayasan Kita Menulis.
- Nuraini, R., Komalasari, R., Kurniawan, F. S., Rachmat, Z., Wahyuddin, S., Munawar, Z., ... Firgia, L. (2023). *Organisasi Dan Arsitektur Komputer*. Global Eksekutif Teknologi.
- Ramadhan, R. F., Wahyuddin, S., Saputri, F. R., Pasaribu, J. S., Almaliki, M. F., Prabiantissa, C. N., ... Darmawan, R. (2023). *Kecerdasan Buatan Digital*. Global Eksekutif Teknologi.
- Wahyuddin, S., Heryana, N., Waworuntu, A., Permana, A. A., Wijayanti, R. R., Pomalingo, S., ... Istiono, W. (2023). *Kontrol Dan Audit Teknologi Informasi*. Global Eksekutif Teknologi.
- Wahyuddin, S., Istiono, W., Rukmana, A. Y., Philip, J., Permana, A. A., Pomalingo, S., ... Adhicandra, I. (2023). *Jaringan komputer*. Get Press Indonesia.
- Wahyuddin, S., Rismayani, R., Sihotang, J. I., Aisa, S., Gunawan, H., Tamsir, N., ... Harlina, S. (2023). *Data Warehouse dan Data Mining*. Yayasan Kita Menulis.
- Wibowo, S. H., Wahyuddin, S., Permana, A. A., Sembiring, S., Wahidin, A. J., Nugroho, J. W., ... Adhicandra, I. (2023). *Teknologi Digital Di Era Modern*. Global Eksekutif Teknologi.

BAB 2

ARSITEKTUR DAN DESAIN IoT

Oleh Dwi Feriyanto

2.1 Pendahuluan

Internet of Thing (IoT) merupakan teknologi berbasis digital yang menghubungkan antara dunia nyata dengan dunia maya. Konsep Teknologi IoT adalah sistem yang mengkoneksikan berbagai perangkat seperti sensor, aktuator, prosesor, maupun perangkat lainnya melalui media internet (Sudianto, Y., 2021). Dengan demikian, IoT dapat dimaknai dengan teknologi yang menghubungkan peralatan di dunia nyata (sensor, aktuator, kamera, dll) ke dunia maya (sosial media, aplikasi khusus) melalui jaringan internet untuk kebutuhan dan gaya hidup manusia.

Dalam perancangan dan pengembangan teknologi, IoT memiliki desain yang memungkinkan manusia untuk menciptakan suatu inovasi yang lebih mutakhir. Desain IoT mencakup prinsip, metode/tahapan, dan platform untuk mengembangkan sistem IoT yang efektif. Desain IoT tersebut dapat diuraikan sebagai berikut:

Prinsip Desain IoT

- Keterhubungan: memastikan perangkat dapat saling terhubung secara *seamless*.
- Skalabilitas: mampu menangani penambahan perangkat dalam jumlah besar.

- Efisiensi Energi: optimalisasi daya perangkat untuk memastikan operasi jangka panjang.
- Keamanan: melindungi data dan perangkat dari ancaman siber.

Tahapan Desain IoT

- Identifikasi kebutuhan: menentukan masalah yang akan diselesaikan oleh solusi IoT.
- Pemilihan perangkat keras berupa sensor dan aktuator yang sesuai dengan aplikasi. Berikutnya pemilihan mikroprosesor/mikrokontroler seperti *Arduino*, *Raspberry Pi*, atau *ESP32*.
- Pemilihan protokol komunikasi: Memilih teknologi jaringan yang sesuai (contoh: Wi-Fi untuk jarak dekat, *LoRa* untuk jarak jauh).
- Pengembangan perangkat lunak: integrasi dengan *platform* IoT seperti *Azure IoT Hub*., antarmuka pengguna (UI) untuk akses data dan kontrol perangkat.

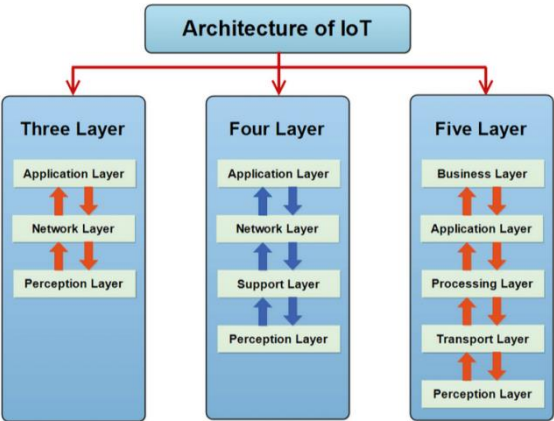
Platform IoT dan Teknologi Pendukung

- Perangkat: *Arduino*, *Raspberry Pi*, *ESP32*.
- Sistem operasi: *Contiki*, *FreeRTOS*, *Zephyr*.
- Protokol IoT: MQTT, CoAP, HTTP/HTTPS.

Begitu pula dalam perancangan dan pengembangan teknologi, IoT memiliki arsitektur yang memungkinkan manusia untuk menciptakan suatu inovasi yang lebih mutakhir. Arsitektur *Internet of Things* (IoT) adalah struktur atau rancangan sistem yang menggambarkan cara perangkat IoT terhubung, berkomunikasi, dan bekerja bersama untuk mencapai tujuan yang diinginkan (Indoboot, 2023). Arsitektur IoT adalah lembar kerja atau *framework* terkait prosedur operasional pengembangan IoT (Edspert, 2023). Dengan demikian dapat dimaknai bahwa arsitektur IoT adalah struktur yang mengatur bagaimana perangkat, sensor, aktuator, dan

layanan *cloud*, saling terhubung dan berinteraksi. Arsitektur ini memungkinkan aliran data dan pertukaran informasi antar perangkat. Arsitektur IoT menggambarkan bagaimana perangkat, jaringan, dan komponen teknologi lainnya berinteraksi dalam sebuah ekosistem IoT.

Terdapat berbagai pandangan tentang jumlah lapisan dalam arsitektur IoT. Jumlah tersebut mulai dari 3, 4 dan 5 lapisan. Perbedaan pandangan di antara para ahli tersebut tidak menjadi masalah, karena pada dasarnya hanya merupakan teori arsitektur yang bertujuan untuk memperjelas konsep dan mekanisme kerja perangkat IoT. Pada kesempatan ini, penulis memilih arsitektur IoT yang berjumlah 4 lapisan, sebab secara konsep telah mewakili secara cerdas dan inovatif.



Gambar 2. 1 Lapisan Arsitektur IoT
(Sumber: <https://shorturl.at/qRMbr>)

2.2 Arsitektur IoT

Adapun arsitektur IoT yang akan disajikan tersebut terdiri atas 4 lapisan/bagian utama. Lapisan tersebut yaitu: *perception layer* (lapisan persepsi), *network layer* (lapisan jaringan), *processing layer* (lapisan pemrosesan), dan *application layer* (lapisan aplikasi). Berikut akan dijelaskan secara lengkap tentang 4 lapisan/bagian dalam arsitektur IoT.

2.2.1 Perception Layer (Lapisan Persepsi)

Perception Layer (lapisan persepsi) adalah bagian terendah dalam arsitektur IoT yang bertugas untuk mengumpulkan data dari lingkungan fisik. Sistem pada lapisan ini, berfokus pada sistem sensor (Tripathy, B.K., & Anuradha, J., 2019). Data ini diperoleh melalui berbagai jenis perangkat seperti sensor dan aktuator, yang menjadi mata dan tangan sistem IoT. Lapisan ini berperan sebagai penghubung antara dunia fisik dan dunia digital/dunia maya.



Gambar 2.2 *Perception Layer* (Lapisan Persepsi)

(Sumber: <https://shorturl.at/qRMbr>)

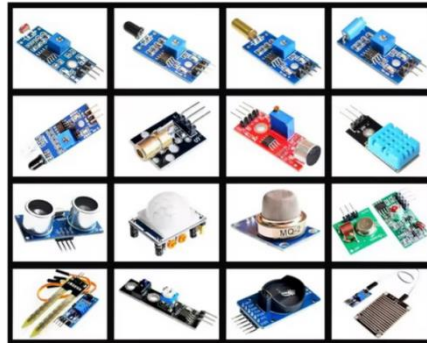
Lapisan Persepsi memiliki 3 fungsi utama yaitu:

- 1) Pengumpulan Data
Komponen lapisan persepsi memperoleh informasi dari lingkungan sekitar, seperti suhu, kelembapan, tekanan, gerakan, posisi, cahaya, atau suara.
- 2) Pemrosesan Awal
Beberapa perangkat di lapisan ini dapat melakukan pemrosesan awal data (*edge computing* sederhana) sebelum mengirimkannya ke lapisan jaringan.
- 3) Pengendalian Lingkungan
Mengontrol lingkungan fisik melalui aktuator berdasarkan instruksi dari sistem IoT.

Komponen utama lapisan persepsi:

- 1) Sensor
Perangkat keras yang mendeteksi perubahan lingkungan fisik dan mengubahnya menjadi sinyal elektronik. Pada kesempatan ini, penulis hanya menyajikan nama dan fungsi sensornya saja,

sedangkan detail tentang sensor dibahas dalam buku yang lain.



Gambar 2. 3 Jenis-Jenis Sensor

(Sumber: <https://shorturl.at/EUzPh>)

Jenis-jenis sensor:

- ✓ Sensor suhu: mengukur perubahan suhu (contoh: DHT22, LM35).
- ✓ Sensor kelembapan: mengukur tingkat kelembapan (contoh: DHT11).
- ✓ Sensor cahaya: mengukur intensitas cahaya (contoh: LDR, TSL2561).
- ✓ Sensor gerak: mendeteksi gerakan (contoh: PIR, *ultrasonic* sensor).
- ✓ Sensor tekanan: memonitor tekanan gas atau cairan (contoh: BMP280).
- ✓ Sensor gas: mendeteksi gas tertentu (contoh: MQ series).

2) Aktuator

Perangkat untuk menerjemahkan keputusan dengan cara mengubah sinyal digital menjadi tindakan fisik atau gerak mekanik, seperti membuka pintu, menyalakan lampu, atau mengontrol motor.



Gambar 2. 4 Jenis Aktuator

(Sumber: <https://shorturl.at/OKu09>)

Jenis-jenis aktuator:

- ✓ Motor (DC, *stepper*, *servo*).
 - ✓ Relay untuk kontrol perangkat listrik.
 - ✓ *Solenoid* untuk kontrol mekanis.
- 3) Kamera dan Perangkat Penginderaan Visual

Kamera adalah alat yang digunakan untuk menangkap gambar atau video dengan cara merekam cahaya yang masuk melalui lensa ke dalam media penyimpanan, seperti film atau sensor digital. Kamera digunakan untuk pengenalan gambar atau video. Berikut contoh alat pengindera visual:

- ✓ Kamera CCTV
- ✓ Kamera thermal.



Gambar 2. 5 Kamera CCTV/Thermal

(Sumber: <https://shorturl.at/hYGQ4>)

4) Robot

Robot adalah mesin yang dirancang untuk melakukan tugas-tugas tertentu secara otomatis atau semi-otomatis dengan sedikit atau tanpa campur tangan manusia. Robot biasanya diprogram untuk melakukan serangkaian perintah atau dapat dikendalikan dari jarak jauh. Robot sering dilengkapi dengan sensor untuk merasakan lingkungan, aktuator untuk bergerak, dan prosesor untuk memproses informasi dan membuat keputusan.



Gambar 2. 6 Robot

(Sumber: <https://shorturl.at/k2bDq>)

Berikut beberapa contoh robot dari berbagai jenis:

- ✓ Robot Industri
- ✓ Robot Servis
- ✓ Robot Militer
- ✓ Robot *Humanoid*
- ✓ Robot *Mobile* dan Otonom
- ✓ Robot Pendidikan dan Penelitian

5) Meter Pengukuran

Meter pengukuran yaitu alat yang digunakan untuk mengukur besaran fisik tertentu, seperti panjang, massa, waktu, suhu, arus listrik, tegangan, dan lainnya. Alat ini membantu mendapatkan nilai kuantitatif yang akurat untuk berbagai keperluan, seperti eksperimen

ilmiah, industri, konstruksi, dan penggunaan sehari-hari. Berikut contoh meter pengukuran:

- ✓ *Meteran*: untuk mengukur panjang atau jarak.
- ✓ *Termometer*: untuk mengukur suhu.
- ✓ *Voltmeter*: untuk mengukur tegangan listrik.
- ✓ *Amperemeter*: untuk mengukur arus listrik.
- ✓ *Timbangan*: untuk mengukur massa atau berat.
- ✓ *Speedometer*: untuk mengukur kecepatan kendaraan.
- ✓ *Hygrometer*: untuk mengukur kelembaban udara.



Gambar 2. 7 Meter Pengukuran Tegangan Listrik

(Sumber: <https://shorturl.at/9yOFN>)

2.2.2 Network Layer (Lapisan Jaringan)

Network Layer (lapisan jaringan) merupakan bagian penting dalam arsitektur IoT yang bertanggung jawab untuk mentransmisikan data dari lapisan persepsi ke pusat pemrosesan atau penyimpanan (*cloud*, *edge*, atau *fog*) dan sebaliknya. Lapisan ini memetakan data dalam jaringan dan memastikan bahwa data atau paket dari perangkat sumber dikirimkan ke perangkat tujuan yang benar (Raj, P., *et al*., 2022). Perangkat tersebut diidentifikasi menggunakan alamat IP-nya, yang ditetapkan dengan menggunakan Protokol Internet (IP) Lapisan ini juga mengelola komunikasi antar perangkat IoT. Fungsi utama lapisan ini adalah memastikan konektivitas yang aman, andal, dan efisien untuk mendukung sistem IoT.



Gambar 2. 8 Lapisan *Network* (Lapisan Jaringan)

(Sumber: <https://shorturl.at/qRMbr>)

Fungsi Utama Lapisan Jaringan sebagai berikut:

- 1) Transmisi Data
 - ✓ Mengirimkan data yang dihasilkan oleh perangkat di lapisan persepsi ke *server* atau *platform* IoT.
 - ✓ Menyediakan saluran komunikasi untuk mengirimkan instruksi kembali ke perangkat (misalnya aktuator).
- 2) Pengelolaan Koneksi
 - ✓ Memastikan konektivitas antar perangkat dengan protokol yang sesuai.
 - ✓ Mendukung berbagai topologi jaringan (*mesh*, *star*, *bus*, dll.)
- 3) Keamanan Komunikasi
 - ✓ Mengamankan transmisi data melalui enkripsi, otentikasi, dan proteksi terhadap serangan *Cyber*.

Komponen Utama Lapisan Jaringan:

- 1) Protokol Komunikasi

Digunakan untuk mengatur cara perangkat IoT berkomunikasi. Beberapa perangkat yang populer meliputi:

 - ✓ *Wi-Fi*: koneksi nirkabel untuk area lokal, yang sering digunakan dalam perangkat pintar. *Wi-Fi* umumnya dapat digunakan untuk berkomunikasi pada jarak hingga 100 meter (Fox, R. & Hao, W., 2017).
 - ✓ *Bluetooth* dan BLE (*Bluetooth Low Energy*): untuk komunikasi jarak dekat dengan konsumsi daya rendah. BLE merupakan radio jarak pendek

dengan daya minimum dan beroperasi dalam jangka waktu cukup lama. Jangkauannya sekitar 100 meter, yang kira-kira 10 kali lebih luas dari *Bluetooth* konvensional. BLE beroperasi menggunakan daya antara 0,01 mW dan 10 mW. Karakteristik ini menjadikan BLE sebagai protokol yang ideal untuk digunakan oleh perangkat IoT (Raj, P., *et al*, 2022).

- ✓ *ZigBee*: protokol hemat daya untuk jaringan *mesh* pada perangkat rumah pintar.
- ✓ *LoRaWAN*: protokol jarak jauh dan hemat daya yang ideal untuk *smart city* atau *smart agriculture*.
- ✓ *NB-IoT* (*Narrowband IoT*): untuk komunikasi berbasis jaringan seluler dengan konsumsi daya rendah.
- ✓ *MQTT* (*Message Queuing Telemetry Transport*): protokol berbasis *publish/subscribe* yang ringan dan cocok untuk IoT.
- ✓ *CoAP* (*Constrained Application Protocol*): protokol *HTTP* ringan untuk perangkat IoT.
- ✓ *AMQP* (*Advanced Messaging Queuing Protocol*): protokol yang menggunakan pesan untuk memungkinkan interaksi antara server dan aplikasi klien.
- ✓ *Cellular* yaitu protokol komunikasi IoT seluler, seperti 4G LTE dan 5G, menawarkan konektivitas jarak jauh yang stabil untuk perangkat IoT.
- ✓ *DDS* (*Data Distribution Service*) merupakan kerangka konektivitas dari *Object Management Group* (OMG) yang dirancang untuk mendukung pertukaran data yang andal, berperforma tinggi, dan kompatibel secara *realtime*.
- ✓ *XMPP* (*Extensible Messaging and Presence Protocol*): dipakai untuk komunikasi berbasis pesan dalam IoT. Protokol ini mendukung

komunikasi dua arah yang ekstensif dan bisa dikonfigurasi untuk berbagai kasus penggunaan yang memerlukan pertukaran pesan *real-time*, seperti dalam sistem otomasi rumah dan interaksi perangkat pintar.

- ✓ LWM2M (*Lightweight Machine to Machine*): protokol ini menyediakan *framework* untuk operasi-operasi seperti pengamatan perangkat, konfigurasi, dan manajemen *firmware* melalui jaringan nirkabel, yang sangat berguna untuk pemeliharaan perangkat IoT yang terdistribusi secara geografis.
- ✓ Z-Wave: sering dimanfaatkan dalam aplikasi *home automation* karena mengutamakan keandalan dan kemudahan penggunaan.

2) Perangkat Jaringan

- ✓ *Gateway IoT*: menghubungkan perangkat di lapisan persepsi dengan *server* atau *cloud*.
- ✓ *Router*: mengarahkan lalu lintas data di jaringan lokal atau internet.
- ✓ *Repeater*: memperluas jangkauan jaringan.
- ✓ 5G/4G

3) Infrastruktur Jaringan

- ✓ Jaringan *Edge*: memproses data lebih dekat ke perangkat untuk mengurangi latensi.
- ✓ Jaringan *Cloud*: penyimpanan dan analisis data skala besar secara terpusat.
- ✓ Jaringan *Fog*: kombinasi *edge* dan *cloud*, memberikan fleksibilitas lebih besar dalam pemrosesan data.
- ✓ 5G/4G

Jenis Teknologi Komunikasi di Lapisan Jaringan:

- ✓ Komunikasi Jarak Pendek
Teknologi yang digunakan yaitu: *Bluetooth*, *BLE*, *ZigBee*, *Z-Wave*.
- ✓ Komunikasi Jarak Menengah
Teknologi yang digunakan yaitu: *Wi-Fi* dan *Ethernet*.
Teknologi ini cocok untuk jaringan lokal yang membutuhkan *bandwidth* tinggi.
- ✓ Komunikasi Jarak Jauh
Teknologi yang digunakan yaitu: *LoRaWAN*, *NB-IoT*, *Sigfox*. Teknologi ini digunakan untuk aplikasi *smart city*, pertanian pintar, dan pengawasan lingkungan.
- ✓ Komunikasi Berbasis Seluler
Teknologi yang digunakan yaitu: 4G/5G, LTE-M.
Teknologi ini ideal untuk aplikasi IoT yang membutuhkan mobilitas tinggi, seperti kendaraan terhubung.

Topologi Jaringan dalam IoT:

- 1) Topologi *Star*
 - ✓ Semua perangkat terhubung langsung ke *gateway* atau hub. pusat.
 - ✓ Keuntungan: mudah dikelola.
 - ✓ Kekurangan: ketergantungan pada hub.
- 2) Topologi *Mesh*
 - ✓ Perangkat saling terhubung dan dapat berbagi data secara langsung.
 - ✓ Keuntungan: lebih tahan terhadap gangguan, efisien untuk jaringan besar.
 - ✓ Kekurangan: konfigurasi lebih kompleks.
- 3) Topologi *Hybrid*
 - ✓ Kombinasi *star* dan *mesh*.
 - ✓ Keuntungan: fleksibilitas lebih tinggi untuk berbagai skala jaringan.

2.2.3 Processing Layer (Lapisan Pemrosesan)

Processing Layer (lapisan pemrosesan) dalam arsitektur IoT bertugas untuk menerima, menyimpan, dan menganalisis data yang dikumpulkan dari lapisan persepsi melalui lapisan jaringan. Arsitektur ini biasanya didasarkan pada perspektif pemrosesan, artinya aliran data mengalir dari *input* ke *output*, untuk melakukan tugas tertentu atau mencapai sasaran target (Sinclair, M., 2017). Hasil dari pemrosesan ini digunakan untuk mengambil keputusan dan mengontrol perangkat IoT atau memberikan informasi kepada pengguna.



Gambar 2.9 Lapisan *Processing* (Lapisan Pemrosesan)

(Sumber: <https://shorturl.at/qRMbr>)

Fungsi Utama Lapisan Pemrosesan yaitu:

- 1) Penyimpanan Data
 - ✓ Menyimpan data yang dihasilkan oleh perangkat IoT untuk digunakan dalam analisis atau referensi di masa depan.
- 2) Pemrosesan dan Analisis Data
 - ✓ Menganalisis data *real-time* atau historis untuk menghasilkan wawasan yang berguna.
 - ✓ Menggunakan algoritma *machine learning*, *big data analytics*, atau kecerdasan buatan (AI).
- 3) Pengelolaan Data
 - ✓ Mengorganisir, memfilter, dan membersihkan data mentah sebelum digunakan lebih lanjut.
- 4) Keamanan Data
 - ✓ Memastikan data aman selama proses penyimpanan dan analisis melalui enkripsi dan autentikasi.

5) Koordinasi Antar Lapisan

- ✓ Mengelola komunikasi dan instruksi antara lapisan aplikasi dan lapisan jaringan.

Komponen Utama Lapisan Pemrosesan:

1) *Edge Computing*

- ✓ Pemrosesan data dilakukan di dekat sumber data, seperti pada perangkat IoT atau *gateway*. Keuntungannya yaitu: latensi lebih rendah, dan mengurangi beban jaringan. Contoh: kamera CCTV pintar yang memproses video langsung untuk mendeteksi gerakan.

2) *Fog Computing*

- ✓ Pemrosesan data dilakukan pada perangkat di antara *edge* dan *cloud*, seperti *router* atau server lokal. Keuntungannya yaitu: kombinasi latensi rendah dan kemampuan pemrosesan lebih tinggi dibandingkan *edge*. Contoh: sistem manajemen lalu lintas pintar yang memproses data dari banyak sensor secara lokal sebelum mengirimnya ke *cloud*.

3) *Cloud Computing*

- ✓ *Cloud Computing* (komputasi awan) pada umumnya mendukung ekosistem IoT dengan berperan sebagai pengumpul data yang diperoleh secara *real-time*, serta sebagai penyedia layanan yang didasarkan pada informasi yang telah dikumpulkan (Sinclair, M., 2017). Pemrosesan dan penyimpanan data dilakukan di pusat data. Keuntungannya yaitu: kapasitas penyimpanan besar dan mendukung analisis data skala besar. Contoh: *platform cloud* seperti *AWS IoT Core*, *Microsoft Azure IoT Hub*, atau *Google Cloud IoT*.

4) *Data Analytics*

- ✓ Analisis data untuk mendeteksi pola, membuat prediksi, atau menghasilkan wawasan. Pendekatan yang digunakan yaitu: *Big Data Analytics* untuk menangani data besar, *machine learning* untuk prediksi berbasis data historis. Analisis waktu nyata untuk aplikasi dengan kebutuhan respons cepat.

5) *Database*

- ✓ Menyimpan data secara terstruktur untuk pemrosesan lebih lanjut. Contoh database antara lain: *SQL: MySQL, PostgreSQL, NoSQL: MongoDB, Cassandra, InfluxDB* untuk data IoT berbasis waktu.

Proses Utama di Lapisan Pemrosesan:

1) *Pengumpulan Data*

- ✓ Data dari lapisan persepsi diterima melalui protokol komunikasi dari lapisan jaringan.

2) *Penyaringan Data*

- ✓ Mengeliminasi data yang tidak relevan atau duplikat untuk meningkatkan efisiensi.

3) *Pemrosesan Data*

- ✓ *Real-time processing*: untuk aplikasi seperti kendaraan otonom atau pemantauan kesehatan. *Batch processing*: untuk analisis data historis yang tidak memerlukan respons instan.

4) *Pengambilan Keputusan*

- ✓ Berdasarkan hasil analisis, sistem menghasilkan keputusan, seperti mengaktifkan aktuator atau mengirim notifikasi kepada pengguna.

2.2.4 **Application Layer (Lapisan Aplikasi)**

Application layer (lapisan aplikasi) adalah bagian tertinggi dalam arsitektur IoT yang menjadi antarmuka antara sistem IoT dan pengguna. Lapisan ini menawarkan beragam layanan sesuai dengan permintaan pelanggan (Raj,

P., *et al.*, 2022). Lapisan ini bertanggung jawab untuk menyampaikan hasil analisis, kontrol, atau wawasan dari data IoT ke pengguna dalam bentuk yang mudah dipahami. Selain itu, lapisan ini juga memungkinkan pengguna untuk mengontrol perangkat IoT melalui antarmuka yang dirancang khusus.



Gambar 2. 10 Lapisan *Application* (Lapisan Aplikasi)

(sumber: <https://shorturl.at/qRMbr>)

Fungsi Utama Lapisan Aplikasi yaitu:

- 1) Penyajian Data
 - ✓ Menyampaikan hasil analisis atau informasi dari lapisan pemrosesan ke pengguna melalui aplikasi atau *dashboard*.
- 2) Interaksi Pengguna
 - ✓ Memberikan antarmuka (*UI/UX*) yang memungkinkan pengguna untuk memantau, mengontrol, atau memberikan instruksi ke sistem IoT.
- 3) Penerjemahan Data
 - ✓ Mengubah data mentah atau hasil analisis menjadi bentuk yang mudah dipahami, seperti grafik, laporan, atau peringatan.
- 4) Penyediaan Layanan
 - ✓ Menyediakan layanan berbasis IoT, seperti monitoring kesehatan, kontrol perangkat rumah pintar, atau manajemen energi.

Komponen Utama Lapisan Aplikasi:

- 1) Aplikasi IoT
 - ✓ Aplikasi berbasis *web*, *desktop*, atau *mobile* yang memungkinkan pengguna berinteraksi dengan sistem IoT. Contoh: aplikasi *smart home* (Google

Home, Alexa), Aplikasi kesehatan wearable (Fitbit, Apple Health).

- 2) Dashboard dan Visualisasi Data
 - ✓ Platform yang menampilkan data dalam bentuk grafik, tabel, atau laporan untuk memantau performa sistem. Contoh: grafana, kibana.
- 3) Notifikasi dan Peringatan
 - ✓ Sistem untuk memberikan peringatan waktu nyata kepada pengguna melalui *email*, SMS, atau aplikasi. Contoh: peringatan detak jantung abnormal dari perangkat kesehatan.
- 4) API (*Application Programming Interface*)
 - ✓ Antarmuka yang memungkinkan aplikasi pihak ketiga untuk mengakses data atau fungsi dari sistem IoT. Contoh: API yang disediakan oleh platform IoT seperti *AWS IoT Core* atau *Google Cloud IoT*.

DAFTAR PUSTAKA

- Sudianto, Y. (2021) 'Desain Arsitektur IoT untuk Budidaya Gurami', *Jurnal Teknologi Informasi dan Ilmu Komputer*, 8(1), p. 111. Available at: <https://doi.org/10.25126/jtiik.0813529>.
- Indoboot. (2023). Mengenal Arsitektur Internet of Things. Diakses tanggal 15-02-2025 pukul 10.09 WIB. Retrieved from <https://blog.indobot.co.id/mengenal-arsitektur-internet-of-things/>
- Edspert. (2023). Kenali Lebih dalam Tentang Arsitektur IoT. Diakses tanggal 15-02-2025 pukul 10.15 WIB. Retrieved from <https://edspert.id/blog/arsitektur-iot/>
- Raj, P., Raman, A.C. and Subramanian, H. (2022). *Cognitive Internet of Things: Enabling Technologies, Platforms, and Use Cases*, *Cognitive Internet of Things: Enabling Technologies, Platforms, and Use Cases*. Available at: <https://doi.org/10.1201/9780429328220>.
- Fox, R. and Hao, W. (2017). *Internet infrastructure: Networking, Web services, and cloud computing*, *Internet Infrastructure: Networking, Web Services, and Cloud Computing*. Available at: <https://doi.org/10.1201/9781315175577>.
- Tripathy, B.K., and Anuradha, J., (2019) *Internet of Things (IoT)*. Available at: <https://doi.org/10.1201/9780429399084>.
- Sinclair, M. (2017) The internet of things, Evidence Based Midwifery.
- Raj, P., Raman, A.C. and Subramanian, H. (2022) *Cognitive Internet of Things: Enabling Technologies, Platforms, and Use Cases*, *Cognitive Internet of Things: Enabling Technologies, Platforms, and Use Cases*. Available at: <https://doi.org/10.1201/9780429328220>.

BAB 3

“THINGS” PADA IoT

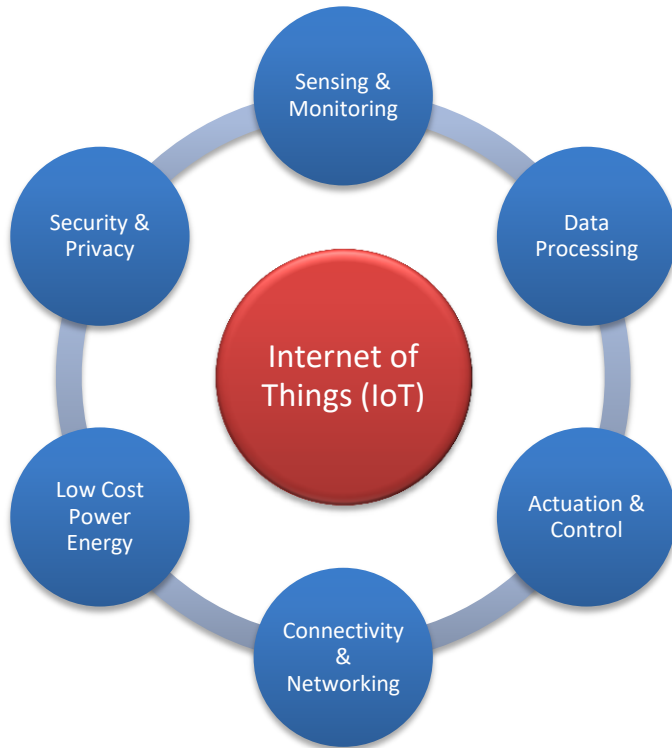
Oleh Dwi Sasmita Aji Pambudi

3.1 Pengertian "Things" dalam IoT

Internet of Things (IoT) merupakan konsep teknologi yang memungkinkan berbagai perangkat fisik untuk saling terhubung melalui jaringan internet, sehingga dapat mengumpulkan, mengirim, dan bertukar data tanpa perlu adanya intervensi manusia secara langsung. Dalam sistem IoT, istilah “*Things*” merujuk pada semua objek fisik yang dapat terhubung ke internet dan memiliki kemampuan untuk berkomunikasi dan berinteraksi dalam jaringan IoT secara otomatis (Kiran, 2019). Objek-objek ini dapat berupa perangkat elektronik, sensor, aktuator, perangkat pintar, kendaraan, peralatan rumah tangga, mesin industri, dan berbagai komponen lain yang telah dilengkapi dengan teknologi komunikasi dan pemrosesan data (Inui *et al.*, 2017). Dengan memahami karakteristik dan kemampuan perangkat yang dapat terhubung, kita dapat mengoptimalkan penggunaan IoT dalam berbagai bidang, seperti otomasi rumah, kesehatan, transportasi, dan manufaktur (Inui *et al.*, 2017).

“*Things*” dalam IoT memiliki karakteristik utama, seperti dapat mengumpulkan data dari lingkungan sekitar menggunakan sensor, memproses informasi dengan unit komputasi yang tertanam (*embedded system*), dan mengambil tindakan melalui aktuator atau sistem kendali otomatis (Kraeling and Brogioli, 2019). Dengan kemampuan ini, perangkat IoT dapat beroperasi secara mandiri atau sebagai

bagian dari sistem yang lebih besar untuk meningkatkan efisiensi dan produktivitas dalam berbagai bidang aplikasi.



Gambar 3. 1 Karakteristik *Things* dalam IoT

(Sumber: Inui et al., 2017)

Perangkat IoT memiliki beberapa karakteristik utama yang membedakannya dari perangkat elektronik biasa, diantaranya yaitu:

1. *Sensing & Monitoring*

Perangkat IoT dilengkapi dengan sensor yang berfungsi untuk mendeteksi dan mengumpulkan data dari lingkungan, seperti suhu, kelembaban, tekanan, gerakan, dan lainnya.

2. *Data Processing*

Data yang dikumpulkan oleh sensor diproses secara lokal (*edge computing*) atau dikirim ke *server/cloud* untuk dianalisis lebih lanjut guna menghasilkan informasi yang berguna.

3. *Actuation & Control*

Selain mengumpulkan data, perangkat IoT juga dapat bertindak berdasarkan hasil analisis, misalnya menghidupkan atau mematikan perangkat lain secara otomatis sesuai dengan kondisi tertentu.

4. *Connectivity & Networking*

IoT membutuhkan koneksi yang handal untuk berkomunikasi antarperangkat dan sistem. Koneksi dapat menggunakan *Wi-Fi, Bluetooth, Zigbee, LoRa*, atau jaringan seluler seperti *4G/5G*.

5. *Low Cost Power Energy*

Perangkat IoT didesain untuk konsumsi daya yang rendah agar dapat bekerja dalam jangka waktu lama, terutama yang menggunakan baterai atau energi terbarukan.

6. *Security & Privacy*

Keamanan data dan privasi pengguna sangat penting dalam IoT. Sistem harus memiliki enkripsi data, autentikasi, serta perlindungan terhadap akses ilegal untuk mencegah serangan siber (Ogonji, Okeyo and Wafula, 2020).

Karakteristik ini menjadikan perangkat IoT lebih cerdas, efisien, dan mampu bekerja secara otomatis dalam berbagai industri dan aplikasi.

3.2 Peran dan Fungsi utama “Things” dalam IoT

Dalam sistem *Internet of Things* (IoT), *Things* atau perangkat fisik berperan sebagai komponen utama yang menghubungkan lingkungan nyata dengan sistem digital. Perangkat ini memungkinkan interaksi antara manusia, mesin,

dan lingkungan melalui pengumpulan data, pemrosesan informasi, dan pengambilan tindakan otomatis(Inui *et al.*, 2017). Berikut adalah beberapa peran dan fungsi utama "*Things*" dalam sistem IoT.

3.2.1 Pengumpulan Data (*Sensing & Monitoring*)

Perangkat IoT menggunakan sensor untuk mendeteksi dan mengumpulkan data dari lingkungan fisik. Sensor ini dapat mengukur berbagai parameter seperti suhu, kelembaban, cahaya, gerakan, tekanan, kualitas udara, dan lainnya. Data yang dikumpulkan kemudian dikirim ke sistem pemrosesan data untuk dianalisis lebih lanjut.

Contoh:

- Sensor suhu & kelembaban dalam sistem pertanian cerdas membantu petani memantau kondisi tanah dan cuaca.
- Sensor kandungan oksigen terlarut (*Dissolved Oxygen*) dan tingkat keasaman (*pH*) dalam sistem budidaya air tawar membantu petambak memantau kondisi air tambak.
- Sensor detak jantung dalam perangkat *wearable* memungkinkan pemantauan kesehatan pengguna secara *real-time*.

3.2.2 Pemrosesan dan Analisis Data (*Edge Computing & Cloud Computing*)

Setelah data dikumpulkan, "*Things*" dalam IoT memproses dan mengelola data secara lokal menggunakan unit pemrosesan tertanam (mikrokontroler) atau mengirimnya ke pusat pemrosesan data di cloud untuk analisis lebih lanjut. Beberapa perangkat hanya berfungsi sebagai pengumpul data, sementara lainnya memiliki kemampuan pemrosesan di tingkat edge computing atau fog computing untuk mengurangi beban pemrosesan di cloud. Dengan pemrosesan data yang lebih efisien, sistem

IoT dapat merespon berbagai kondisi secara real-time tanpa menunggu perintah dari server pusat (Wolf, 2023).

Contoh:

- *Smart thermostat* dapat mempelajari pola penggunaan suhu di rumah dan menyesuaikan pengaturan pendingin atau pemanas secara otomatis.
- Kamera keamanan berbasis AI dapat memproses rekaman video untuk mendeteksi pergerakan mencurigakan sebelum mengirim peringatan ke pengguna.
- *Smart grid / smart power* menganalisis pola konsumsi listrik dan menyesuaikan distribusi energi secara otomatis untuk meningkatkan efisiensi serta mengurangi pemborosan daya. Selain itu, sistem ini dapat mendeteksi gangguan jaringan listrik lebih cepat dan mengoptimalkan penggunaan energi terbarukan seperti tenaga surya dan angin (Qays *et al.*, 2023).

3.2.3 Pengambilan Keputusan & Automasi (*Actuation & Control*)

Perangkat IoT dapat mengambil tindakan berdasarkan hasil analisis data yang diperoleh, baik secara otomatis maupun melalui perintah pengguna. Perangkat IoT dapat mengambil tindakan otomatis melalui aktuator. Hal ini memungkinkan sistem dapat bekerja tanpa perlu campur tangan (intervensi) manusia secara langsung.

Contoh:

- Sistem irigasi otomatis di bidang pertanian akan mengaktifkan penyiraman hanya ketika kelembaban tanah berada di bawah ambang batas tertentu.
- Sensor gerak (*motion sensor*) dalam sistem *smart home*, seperti sensor PIR, radar, ultrasonik, dan lainnya dapat mendeteksi keberadaan seseorang di dalam ruangan dan secara otomatis menyalakan lampu atau mengatur suhu ruangan.

- Aktuator (dalam sistem industri) dapat mengontrol mesin berdasarkan data operasional untuk meningkatkan efisiensi produksi.
- Sistem budidaya tambak otomatis di bidang perikanan akan mengaktifkan kincir air (sistem aerasi) hanya ketika tingkat kandungan oksigen terlarut dalam air berada di bawah level tertentu untuk menjaga kualitas air untuk keberlangsungan hidup ikan atau udang.
- Sistem pintu air otomatis di bidang pengairan akan membuka atau menutup pintu air berdasarkan tingkat ketinggian air yang terdeteksi oleh sensor untuk mencegah terjadinya banjir.

3.2.4 Komunikasi dan Pertukaran Data dalam Sistem IoT (*Connectivity & Networking*)

Perangkat IoT harus dapat berkomunikasi dengan sistem lain melalui berbagai teknologi jaringan seperti *Wi-Fi*, *Bluetooth*, *Zigbee*, *LoRa*, atau *5G*. Protokol komunikasi ini memastikan data dapat ditransfer dengan cepat dan aman.

Contoh:

- Mobil otonom menggunakan sensor IoT dan komunikasi 5G untuk berinteraksi dengan infrastruktur lalu lintas dan kendaraan lain di sekitarnya.
- *Smartwatch* dapat mengirim data kesehatan pengguna ke aplikasi di *smartphone* untuk pemantauan jarak jauh.

3.3 Optimalisasi Kinerja "*Things*" dalam Sistem IoT

Optimalisasi kinerja "*Things*" dalam sistem IoT bertujuan untuk meningkatkan efisiensi, keandalan, dan keamanan perangkat dalam mengumpulkan, memproses, serta bertukar data. Hal ini dapat dicapai melalui pemilihan sensor dan aktuator yang tepat, penerapan *edge computing* untuk mengurangi latensi, serta penggunaan teknologi hemat daya seperti *Low Power Wide Area Network (LPWAN)*. Selain itu,

optimalisasi jaringan dengan protokol komunikasi yang efisien (seperti *MQTT* dan *CoAP*), serta penerapan keamanan berbasis enkripsi dan autentikasi, sangat penting untuk melindungi data dan sistem dari ancaman siber. Pemeliharaan prediktif dengan *Artificial Intelligence (AI)* juga membantu mencegah kegagalan perangkat sebelum terjadi, sedangkan standarisasi dan interoperabilitas memastikan perangkat dari berbagai pabrikan dapat bekerja secara harmonis dalam ekosistem IoT yang luas (Kraeling and Brogioli, 2019).

3.3.1 Integrasi dengan Sistem Lain dan Ekosistem Digital

IoT memungkinkan berbagai perangkat untuk terhubung dan bekerja bersama dalam satu ekosistem, seperti integrasi dengan AI (*Artificial Intelligence*), *Big Data*, dan *Blockchain* untuk meningkatkan efisiensi dan keamanan (Adere, 2022; Gopal, Poongodi and Nanthiya, 2022; Mathur *et al.*, 2023).

Contoh:

- Rumah pintar (*smart home*) dapat mengintegrasikan pencahayaan, keamanan, dan suhu dalam satu sistem yang dikendalikan melalui *virtual assistant* seperti *Google Assistant* atau *Alexa*.
- Sistem manajemen kota cerdas (*smart city*) dapat menggunakan IoT untuk mengatur lampu lalu lintas, parkir otomatis, dan pemantauan kualitas udara dalam satu platform terpusat.

3.3.2 Efisiensi Energi dan Pengelolaan Sumber Daya

Perangkat IoT sering dirancang untuk menggunakan energi secara efisien, terutama yang berbasis baterai atau sumber daya terbatas. Teknologi seperti *sleep mode*, *edge computing*, dan jaringan hemat energi (*LPWAN*) digunakan untuk optimalisasi konsumsi daya.

Contoh:

- Sensor IoT di ladang minyak dan gas memantau kondisi peralatan dan hanya mengirimkan data ketika terjadi perubahan signifikan, sehingga menghemat konsumsi daya komunikasi.
- *Smart meter* listrik dapat menganalisis pola konsumsi energi dan membantu pengguna menghemat biaya listrik.

3.3.3 Meningkatkan Keamanan dan Pengawasan (*Security and Surveillance*)

IoT digunakan untuk meningkatkan keamanan melalui sistem pemantauan berbasis sensor dan kamera yang dapat mendeteksi ancaman atau kejadian mencurigakan (Kala and Nalesh, 2022).

Contoh:

- *CCTV* berbasis *AI* dapat mengenali wajah dan mengirim notifikasi saat ada orang yang tidak dikenal memasuki area tertentu.
- Sistem keamanan rumah pintar menggunakan sensor gerak dan *alarm* otomatis yang terhubung dengan aplikasi *mobile* pemilik rumah.

3.3.4 Peningkatan Efisiensi Operasional dalam Sektor Industri dan Bisnis

Di sektor industri dan bisnis, IoT membantu mengotomatiskan proses operasional, mengurangi biaya, meningkatkan produktivitas.

Contoh:

- Robot berbasis IoT di gudang logistik secara otomatis mengambil & menyusun barang, mempercepat pengiriman.
- Sensor pada mesin industri memungkinkan pemantauan kondisi mesin secara *real-time*, mencegah kerusakan sebelum terjadi (*predictive maintenance*).

3.3.5 Memberikan Pengalaman Pengguna dengan Lebih Baik (*User Experience & Personalization*)

IoT memungkinkan interaksi yang lebih cerdas dengan pengguna, memberikan pengalaman yang lebih personal dan sesuai dengan kebutuhan individu.

Contoh:

- *Virtual Assistant* berbasis IoT, seperti *Siri* atau *Alexa*, dapat memahami kebiasaan pengguna dan memberikan rekomendasi otomatis.
- Mobil pintar dapat menyesuaikan pengaturan kursi dan suhu berdasarkan preferensi pengemudi.

3.3.6 Mendukung *Smart Cities* dan Keberlanjutan Lingkungan

IoT berperan dalam pengelolaan lingkungan & pembangunan kota cerdas, membantu menciptakan solusi yang lebih berkelanjutan dan ramah lingkungan (Panahi Rizi and Hosseini Seno, 2022).

Contoh:

- Sistem pemantauan kualitas udara di kota cerdas dapat mendeteksi polusi dan memberikan rekomendasi kepada warga untuk menghindari area tertentu.
- Pengelolaan sampah berbasis IoT memungkinkan penjadwalan pengangkutan sampah berdasarkan kapasitas tempat sampah, mengurangi konsumsi bahan bakar kendaraan pengangkut sampah.

3.4 Klasifikasi "*Things*" dalam Sistem IoT

Perangkat atau objek "*Things*" terhubung dengan internet dan memungkinkan interaksi serta pertukaran data dengan sistem lain secara *real-time*. Dengan adanya "*Things*" dalam IoT, sistem dapat mengotomatisasi proses, meningkatkan efisiensi operasional, serta mendukung pengambilan keputusan berbasis data.

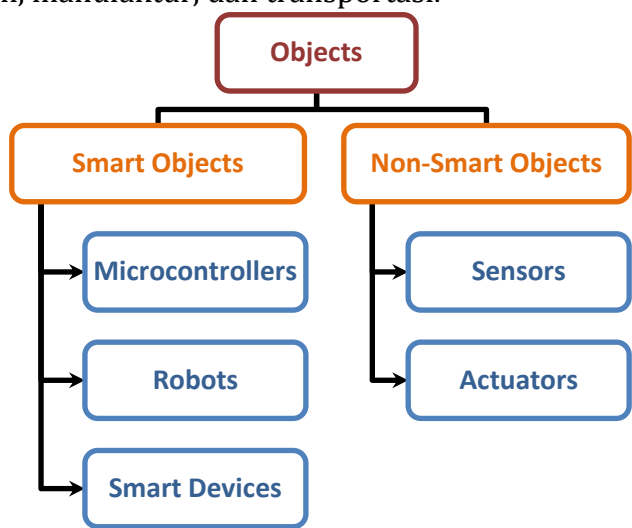
Komponen "*Things*" dalam IoT berperan penting dalam mengumpulkan data dari lingkungan sekitar, memproses informasi yang diperoleh, dan berkomunikasi dengan perangkat lain atau *server* pusat. Data yang dikumpulkan kemudian dianalisis untuk menghasilkan tindakan yang dapat diotomatisasi, baik dalam skala kecil seperti perangkat rumah pintar (*smart home*) maupun dalam skala besar seperti sistem industri, transportasi, dan kesehatan (Inbamani *et al.*, 2022).

Berdasarkan fungsinya, "*Things*" dalam IoT dapat dikategorikan menjadi dua jenis utama, yaitu:

1. Objek Cerdas (*Smart Objects*), yaitu objek atau perangkat yang memiliki kecerdasan buatan atau kemampuan pemrosesan data secara mandiri sehingga dapat mengambil keputusan sendiri berdasarkan data yang dikumpulkan dan berinteraksi dengan sistem lain tanpa campur tangan manusia secara langsung. Perangkat ini biasanya dilengkapi dengan unit pemrosesan yang memungkinkan mereka untuk beradaptasi terhadap kondisi lingkungan serta berkomunikasi dengan perangkat lain dalam sistem IoT.
2. Objek Non-Cerdas (*Non-Smart Objects*), yaitu perangkat fisik yang tidak memiliki kecerdasan dan kemampuan pemrosesan data sendiri, tetapi tetap dapat berfungsi dan diintegrasikan dalam sistem IoT dengan bantuan perangkat tambahan. Objek ini hanya berfungsi sebagai media pasif yang menyediakan data atau dipengaruhi oleh keputusan sistem yang lebih cerdas.

Dengan memahami klasifikasi ini, kita dapat mengidentifikasi bagaimana perangkat-perangkat tersebut berperan dalam membangun sistem IoT yang lebih efisien, terhubung, dan mampu meningkatkan produktivitas di berbagai sektor. Pengidentifikasian perangkat "*Things*" dalam IoT mampu memastikan integrasi yang efisien, interoperabilitas, serta keamanan sistem. Dengan mengelompokkan perangkat berdasarkan fungsi dan karakteristiknya, sistem dapat mengoptimalkan pemanfaatan sensor, aktuator, dan perangkat

komunikasi dalam berbagai aplikasi industri. Identifikasi perangkat juga berperan dalam meningkatkan keamanan dengan mencegah akses ilegal, mempermudah pemeliharaan, serta mendukung pengelolaan data yang lebih efisien. Selain itu, klasifikasi ini memungkinkan sistem IoT untuk berkembang secara *scalable*, mempermudah ekspansi tanpa mengganggu perangkat yang sudah ada, serta menyesuaikan implementasi IoT dengan kebutuhan spesifik di berbagai sektor, seperti kesehatan, manufaktur, dan transportasi.



Gambar 3. 2 Klasifikasi Objek "Things"
(Sumber :GeeksforGeeks, 2020)

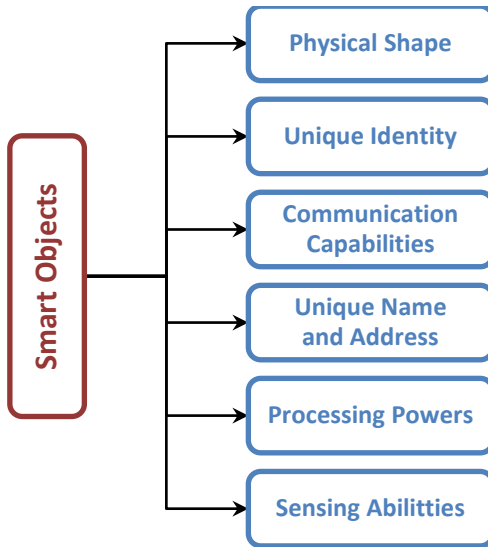
3.4.1 Objek Cerdas (*Smart Objects*)

Objek cerdas memiliki kecerdasan atau kemampuan untuk beradaptasi dan berinteraksi dengan lingkungannya. Seiring dengan perkembangan teknologi, banyak perangkat sehari-hari yang telah berevolusi menjadi objek cerdas yang mampu berkomunikasi, bereaksi, dan mengenali objek lain di sekitarnya berdasarkan kondisi lingkungan.

Objek cerdas merupakan objek fisik dan digital yang dapat diidentifikasi, memiliki kemampuan sensor atau aktuasi, dapat melakukan pemrosesan dan perhitungan,

serta memiliki kapasitas penyimpanan dan konektivitas jaringan. Objek cerdas memiliki beberapa karakteristik khusus yang membedakannya dari objek biasa. Berikut adalah beberapa karakteristik utama yang dimiliki oleh objek cerdas.

1. Bentuk Fisik (*Physical Shape*)
Objek cerdas harus memiliki bentuk fisik yang memungkinkan untuk ditempatkan dalam suatu infrastruktur atau lingkungan tertentu.
2. Identitas Unik (*Unique Identifier*)
Objek cerdas harus memiliki identitas unik yang membedakannya dari objek lain dalam sistem. Identitas ini dapat digunakan untuk pelacakan dan identifikasi dalam sistem IoT.
3. Kemampuan Komunikasi (*Communication Capabilities*)
Salah satu aspek utama dari objek cerdas adalah kemampuannya untuk mengirim dan menerima data melalui internet atau teknologi jaringan lainnya.
4. Nama dan Alamat Unik (*Unique Name and Address*)
Setiap objek cerdas harus memiliki alamat unik dalam jaringan, seperti alamat IP, untuk memungkinkan komunikasi dan integrasi yang efisien dalam sistem IoT.
5. Kemampuan Pemrosesan (*Processing Powers*)
Objek cerdas memiliki kemampuan komputasi dan pemrosesan untuk membuat keputusan berdasarkan data yang dikumpulkan.
6. Kemampuan Sensor (*Sensing Capabilities*)
Objek cerdas sering dilengkapi dengan sensor untuk mengumpulkan informasi dari lingkungannya, seperti suhu, tekanan, atau keberadaan zat berbahaya.



Gambar 3. 3 Karateristik Objek Cerdas (*Smart Objects*)
(Sumber : (GeeksforGeeks, 2020))

Konsep utama dari *Internet of Things* (IoT) adalah mengurangi ketergantungan terhadap intervensi manusia dalam berbagai sistem, dan objek cerdas berperan penting dalam mewujudkan tujuan ini. Oleh karena itu, objek cerdas sering disebut sebagai komponen utama atau "*building blocks*" dalam sistem IoT. Hubungan antara objek cerdas dan IoT dapat dianalogikan sebagai dua roda kendaraan yang bekerja bersama untuk mempercepat transformasi infrastruktur modern.

Di sekitar kita, banyak perangkat yang telah menjadi objek cerdas berkat perkembangan teknologi. Contohnya, hampir semua orang memiliki smartphone di saku mereka. Selain itu, perangkat seperti kulkas pintar (*smart fridge*), TV pintar (*smart TV*), dan asisten suara seperti *Alexa* adalah beberapa contoh teknologi modern yang sering kita gunakan. Mikrokontroler seperti Arduino juga merupakan contoh perangkat cerdas yang banyak

digunakan dalam berbagai aplikasi IoT. Beberapa contoh umum dari objek cerdas meliputi:

- *Smartphone*
Perangkat yang mendukung berbagai fungsi cerdas seperti pengenalan wajah, pemantauan lokasi, konektivitas yang luas.
- Perangkat Rumah Pintar
Seperti lampu pintar (*smart light*), ac pendingin pintar (*smart air conditioner*), dan kamera keamanan berbasis kecerdasan buatan (AI) yang dapat dikendalikan dari jarak jauh melalui aplikasi atau perintah suara, serta menyesuaikan pengoperasiannya secara otomatis berdasarkan kondisi lingkungan dan preferensi pengguna.
- Peralatan Industri
Robot otomatis dalam manufaktur yang dapat menyesuaikan operasi kerjanya berdasarkan kumpulan data yang diterima.
- Perangkat Kesehatan
Smartwatch dan perangkat medis lainnya yang memantau detak jantung, kadar oksigen dalam darah, dan aktivitas fisik pengguna.

3.4.2 Objek Non-Cerdas (*Non-Smart Objects*)

Objek non-cerdas merupakan benda atau perangkat yang tidak memiliki kecerdasan buatan maupun kemampuan pemrosesan data secara mandiri. Perangkat ini tidak dapat berkomunikasi atau melakukan analisis sendiri, tetapi dapat menjadi bagian dari sistem IoT dengan bantuan teknologi tambahan seperti sensor dan aktuator.

Objek ini berperan sebagai elemen pasif dalam sistem, di mana fungsinya terbatas pada penyediaan data tanpa kemampuan untuk menganalisis atau mengambil keputusan sendiri. Keberadaannya bergantung pada sistem yang lebih cerdas, yang akan memproses informasi yang

diberikan dan menentukan tindakan yang sesuai. Dengan kata lain, objek ini tidak memiliki kendali atas operasionalnya sendiri, melainkan hanya merespons instruksi atau perubahan yang terjadi dalam sistem IoT.

Meskipun tidak memiliki kemampuan pemrosesan sendiri, objek ini tetap dapat diintegrasikan ke dalam sistem IoT dengan bantuan sensor eksternal, aktuator, atau tag identifikasi seperti *RFID* (*Radio Frequency Identification*), yang memungkinkan mereka untuk berinteraksi dengan lingkungan dan sistem yang lebih cerdas.

Beberapa contoh umum dari objek non-cerdas pada berbagai aplikasi IoT dengan bantuan teknologi pendukung, diantaranya:

1. Pakaian atau Sepatu dengan Sensor
Objek ini hanya menjadi "cerdas" ketika dihubungkan dengan perangkat pintar yang dapat mengumpulkan dan memproses data.
2. Rak Gudang dengan *RFID*
Meskipun rak penyimpanan tidak memiliki kemampuan pemrosesan sendiri, *tag RFID* (*Radio Frequency Identification*) memungkinkan pelacakan inventaris secara otomatis dalam sistem logistik.
3. Kontainer Logistik
Kontainer pengiriman yang dilengkapi dengan sensor *GPS* (*Global Positioning System*) atau sensor suhu eksternal dapat dipantau untuk memastikan keamanan dan kondisi barang selama pengiriman.

Memahami perbedaan antara objek cerdas dan non-cerdas memungkinkan kita lebih mudah mengidentifikasi perangkat yang memerlukan tambahan teknologi agar dapat diintegrasikan ke dalam sistem IoT. Kombinasi objek cerdas, sensor, dan aktuator memastikan IoT berfungsi secara optimal, mengurangi kebutuhan intervensi manusia,

serta membuka peluang baru dalam berbagai industri dan sektor kehidupan.

3.5 Sensor dan Aktuator sebagai Bagian dari IoT

Dalam sistem *Internet of Things* (IoT), *Things* merujuk pada objek fisik yang terhubung ke jaringan dan dapat berinteraksi dengan lingkungan sekitarnya. Agar *Things* dapat berfungsi secara cerdas, diperlukan sensor dan aktuator sebagai komponen utama.

Sensor berperan dalam mengumpulkan data dari lingkungan, seperti suhu, kelembaban, cahaya, atau gerakan. Data ini kemudian dikirim ke sistem pemrosesan untuk dianalisis. Sedangkan aktuator bertindak berdasarkan data yang diterima, misalnya menghidupkan lampu secara otomatis, mengontrol suhu ruangan, atau mengaktifkan alarm keamanan. Dengan dukungan sensor dan aktuator, sistem IoT dapat bekerja secara otomatis, meningkatkan efisiensi, serta mempermudah pengambilan keputusan tanpa memerlukan intervensi manusia secara langsung.

Sensor dan aktuator memiliki peran penting dalam sistem IoT. Dengan kombinasi sensor dan aktuator, objek non-cerdas dapat diubah menjadi bagian dari sistem IoT yang lebih cerdas dan responsif terhadap lingkungan sekitar. Berikut adalah penjelasan singkat tentang masing-masing komponen.

1. Sensor merupakan perangkat elektronik yang terdiri dari sel-sel sensitif dan memiliki kemampuan untuk mendeteksi dan mengukur parameter fisik tertentu. Sensor berfungsi sebagai alat untuk menangkap perubahan lingkungan, dengan mengubah fenomena fisik seperti suhu, tekanan, kelembaban, atau konsentrasi gas beracun, lalu mengubahnya menjadi sinyal listrik yang dapat diproses oleh sistem elektronik lainnya. Data dari sensor digunakan untuk pengambilan keputusan dalam sistem IoT. Contoh sensor yang sering digunakan dalam IoT meliputi :
 - Sensor Suhu (DHT11, DS18B20)

- Sensor Kelembaban (DHT22, HIH-4000)
 - Sensor Tekanan (BMP180, MPX5010)
 - Sensor Proksimitas (Ultrasonik, Inframerah)
 - Sensor Gas (MQ-2, MQ-135)
 - Sensor Cahaya (LDR, TSL2561)
2. Aktuator merupakan perangkat yang berfungsi untuk menjalankan perintah dengan melakukan aksi atau tugas tertentu berdasarkan informasi yang diterima dari sensor atau sistem pemrosesan data. Aktuator dapat bekerja dengan mengubah sinyal elektronik menjadi gerakan mekanis, perubahan posisi, atau tindakan lain sesuai dengan kebutuhan sistem. Terdapat dua jenis aktuator utama, yaitu:
- Aktuator Mekanik adalah aktuator yang bekerja dengan menghasilkan gerakan fisik serta mengendalikan pergerakan atau mekanisme tertentu. Contohnya termasuk motor dc, servo, stepper dalam robotika & otomasi, motor listrik dalam mesin industri, katup (*valve*) solenoid otomatis dalam sistem perpipaan dan kontrol aliran gas atau fluida.
 - Aktuator Digital adalah aktuator yang berfungsi menjalankan tugas atau melakukan tindakan berbasis perangkat lunak yang dipicu oleh sensor dalam sistem IoT, seperti pengiriman email otomatis, notifikasi getaran pada perangkat mobile, atau mengaktifkan peringatan keamanan.

3.5.1 Sensor Suhu (*Temperature Sensor*)

Sensor suhu adalah perangkat yang digunakan untuk mengukur suhu lingkungan atau suatu objek. Sensor ini bekerja dengan mendeteksi perubahan suhu dan mengubahnya menjadi sinyal listrik yang dapat dianalisis oleh sistem elektronik.

Sensor suhu beroperasi berdasarkan perubahan karakteristik fisik akibat variasi suhu. Misalnya, sensor

termistor mengalami perubahan resistansi seiring dengan perubahan suhu, sedangkan sensor berbasis semikonduktor mengubah suhu menjadi tegangan listrik yang dapat diukur. Beberapa jenis sensor suhu, diantaranya :

- DHT11 yaitu sensor suhu dan kelembaban dengan akurasi sedang, sering digunakan dalam proyek IoT.
- DS18B20 yaitu sensor suhu digital dengan akurasi tinggi, dapat digunakan dalam lingkungan ekstrem seperti di industri dan laboratorium.

Beberapa contoh aplikasi penggunaan dari sensor suhu, diantaranya:

- Sistem HVAC, sensor digunakan untuk mengontrol suhu dalam sistem pemanas, ventilasi, dan pendingin udara.
- Pemantauan Cuaca, sensor digunakan dalam stasiun cuaca untuk memantau perubahan suhu lingkungan.
- Industri Makanan, sensor digunakan untuk memastikan suhu penyimpanan makanan tetap sesuai standar keamanan pangan.
- Peralatan Medis, sensor digunakan dalam termometer digital untuk mengukur suhu tubuh pasien.

3.5.2 Sensor Kelembaban (*Humidity Sensor*)

Sensor kelembaban adalah perangkat yang digunakan untuk mengukur kadar uap air dalam udara atau lingkungan tertentu. Sensor ini sering digunakan dalam aplikasi yang memerlukan pemantauan kelembaban, seperti pertanian, industri, & sistem HVAC.

Sensor kelembaban bekerja dengan mendeteksi perubahan sifat listrik atau mekanik akibat kadar uap air di udara. Sensor ini mengubah perubahan tersebut menjadi sinyal listrik yang dapat diinterpretasikan oleh sistem pemrosesan data.

Beberapa jenis sensor kelembaban, diantaranya:

- DHT22 yaitu sensor kelembaban digital dengan akurasi lebih tinggi dibandingkan DHT11, sering digunakan dalam sistem pemantauan lingkungan.
- HIH-4000 yaitu sensor kelembaban kapasitif dengan respons cepat, banyak digunakan dalam industri dan aplikasi medis.

Beberapa contoh aplikasi penggunaan dari sensor kelembaban, diantaranya:

- Pertanian Cerdas, sensor digunakan dalam sistem irigasi otomatis untuk menjaga kelembaban tanah.
- Penyimpanan Produk, sensor digunakan dalam gudang penyimpanan makanan atau farmasi untuk memastikan kadar kelembaban tetap optimal.
- Sistem HVAC, sensor digunakan untuk membantu mengontrol kelembaban dalam ruangan agar tetap nyaman bagi penghuni.

3.5.3 Sensor Tekanan (*Pressure Sensor*)

Sensor tekanan adalah perangkat yang digunakan untuk mengukur tekanan gas atau cairan dalam suatu sistem. Sensor ini bekerja dengan mendeteksi perubahan tekanan dan mengubahnya menjadi sinyal listrik yang dapat dianalisis lebih lanjut.

Sensor tekanan bekerja dengan mendeteksi perubahan gaya yang diberikan oleh gas atau cairan pada elemen sensor. Perubahan ini kemudian dikonversi menjadi sinyal listrik yang sesuai dengan nilai tekanan.

Beberapa jenis sensor tekanan, diantaranya:

- BMP180 yaitu sensor tekanan digital yang sering digunakan dalam altimeter dan stasiun cuaca.
- MPX5010 yaitu sensor tekanan analog dengan sensitivitas tinggi, sering digunakan dalam aplikasi medis dan industri.

Beberapa contoh aplikasi penggunaan dari sensor tekanan, diantaranya:

- Sistem Pemantauan Cuaca, sensor digunakan dalam altimeter dan barometer untuk mengukur tekanan atmosfer.
- Industri Otomotif, sensor digunakan dalam sistem pemantauan tekanan ban (TPMS).
- Aplikasi Medis, sensor digunakan dalam alat pengukur tekanan darah otomatis.

3.5.4 Sensor Proksimitas (*Proximity Sensor*)

Sensor Proksimitas adalah sensor yang digunakan untuk mendeteksi keberadaan atau kedekatan suatu objek tanpa menyentuhnya secara fisik, sehingga dapat mengurangi keausan dan meningkatkan efisiensi operasional.

Sensor ini bekerja berdasarkan berbagai prinsip, seperti medan elektromagnetik, cahaya, atau gelombang ultrasonik, untuk mengidentifikasi objek dalam jarak tertentu. Sensor Proksimitas bekerja dengan mengeluarkan sinyal (misalnya, gelombang elektromagnetik atau ultrasonik) dan mendeteksi perubahan yang terjadi akibat keberadaan objek. Jika ada objek yang berada dalam jangkauan sensor, sinyal tersebut akan dipantulkan kembali dan dianalisis untuk menentukan jarak atau keberadaan objek tersebut.

Beberapa jenis sensor proksimitas, diantaranya:

- Sensor Induktif digunakan untuk mendeteksi objek berbahan logam, dan memanfaatkan medan elektromagnetik.
- Sensor Kapasitif mampu mendeteksi objek berbahan logam dan non-logam berdasarkan perubahan kapasitansi.
- Sensor Ultrasonik menggunakan gelombang ultrasonik untuk mendeteksi objek, sering digunakan dalam sistem parkir kendaraan.

- Sensor Inframerah (IR) menggunakan cahaya inframerah untuk mendeteksi objek berdasarkan pantulan sinyal.

Beberapa contoh aplikasi penggunaan dari sensor proksimitas diantaranya:

- Otomotif, sensor digunakan dalam sistem parkir kendaraan untuk mendeteksi objek di sekitar mobil.
- Manufaktur & Otomasi, sensor digunakan dalam mesin produksi untuk mendeteksi posisi benda kerja.
- Perangkat *Mobile*, sensor dipasang pada smartphone untuk mendeteksi saat pengguna mendekatkan wajah ke layar (misalnya, saat melakukan panggilan telepon).
- Keamanan, sensor digunakan dalam sistem *alarm* dan akses pintu otomatis.

3.5.5 Sensor Gas (Gas Sensor)

Sensor gas adalah perangkat yang digunakan untuk mendeteksi keberadaan gas tertentu dalam suatu lingkungan. Sensor ini sering digunakan dalam sistem keamanan dan industri untuk mendeteksi gas beracun atau kebocoran gas.

Sensor gas bekerja dengan mendeteksi perubahan resistansi atau reaksi kimia akibat interaksi gas dengan elemen sensor. Hasil deteksi ini dikonversi menjadi sinyal listrik yang dapat digunakan untuk analisis lebih lanjut.

Beberapa jenis sensor gas, diantaranya:

- MQ-2, yaitu sensor gas yang mampu mendeteksi asap, LPG, metana, dan karbon monoksida.
- MQ-135, yaitu sensor yang digunakan untuk mendeteksi berbagai gas berbahaya di udara, seperti amonia (NH_3), benzena, karbon dioksida (CO_2), dan gas-gas organik lainnya, sering digunakan dalam sistem pemantauan kualitas udara.

Beberapa contoh aplikasi penggunaan dari sensor gas, diantaranya:

- Sistem Keamanan Rumah, sensor digunakan untuk mendeteksi kebocoran gas di dapur atau garasi.
- Industri Manufaktur, sensor digunakan untuk mendeteksi gas beracun di area produksi.
- Pemantauan Lingkungan, sensor digunakan dalam sistem deteksi polusi udara.

3.5.6 Sensor Cahaya (*Light Sensor*)

Sensor cahaya adalah perangkat yang digunakan untuk mengukur intensitas cahaya dalam suatu lingkungan. Sensor ini sering digunakan dalam sistem otomatisasi yang bergantung pada perubahan kondisi pencahayaan.

Sensor cahaya bekerja dengan mendeteksi jumlah cahaya yang diterima dan mengubahnya menjadi sinyal listrik. Sensor berbasis fotodiode atau LDR (*Light Dependent Resistor*) mengubah resistansinya berdasarkan jumlah cahaya yang diterima.

Beberapa jenis sensor cahaya, diantaranya:

- LDR (*Light Dependent Resistor*), yaitu sensor sederhana yang mengubah resistansi berdasarkan intensitas cahaya yang diterima.
- TSL2561, yaitu sensor cahaya digital dengan kemampuan pengukuran yang lebih akurat.

Beberapa contoh aplikasi penggunaan dari sensor cahaya, diantaranya:

- Penerangan Otomatis, sensor digunakan dalam sistem pencahayaan yang menyesuaikan intensitas cahaya secara otomatis.
- Kamera Digital, sensor digunakan dalam sistem eksposur otomatis pada kamera.
- Pemantauan Lingkungan, sensor digunakan untuk mengukur tingkat pencahayaan dalam sistem pertanian, penelitian astronomi, maupun kontrol panel surya dalam mengoptimalkan penyerapan energi matahari.

3.5.7 Aktuator

Dalam sistem *Internet of Things* (IoT), aktuator bertindak sebagai eksekutor yang menjalankan respons terhadap data yang dikumpulkan oleh sensor, memungkinkan sistem bekerja secara otomatis tanpa campur tangan manusia.

Aktuator menerima sinyal atau perintah dari mikrokontroler, komputer, atau sistem kontrol lainnya. Perintah ini kemudian dikonversi menjadi aksi fisik seperti gerakan mekanis, perubahan suhu, atau perubahan kondisi lainnya. Misalnya, dalam sistem pendingin otomatis, sensor suhu mendeteksi panas yang berlebih, lalu aktuator kipas menyala untuk menurunkan suhu ruangan.

Beberapa jenis aktuator, diantaranya:

1. Aktuator Mekanik menghasilkan gerakan fisik untuk mengontrol pergerakan atau mekanisme tertentu.
Contoh: Motor servo dalam robotika, motor listrik dalam conveyor belt, atau katup otomatis dalam sistem perpipaan.
2. Aktuator Elektrik bekerja dengan mengubah energi listrik menjadi gerakan atau perubahan lain yang diinginkan.
Contoh: Solenoid yang digunakan untuk membuka dan menutup kunci pintu otomatis, relay yang digunakan untuk pengendalian perangkat berdaya tinggi dengan menggunakan sinyal berdaya rendah.
3. Aktuator Hidrolik menggunakan tekanan fluida (minyak atau air) untuk menghasilkan tenaga dan gerakan yang kuat.
Contoh: Sistem rem hidrolik pada kendaraan atau lengan robot hidrolik di industri.
4. Aktuator Pneumatik bekerja dengan menggunakan udara bertekanan untuk menghasilkan gerakan mekanis.

Contoh: Pintu otomatis di pusat perbelanjaan atau sistem penggerak dalam lini produksi industri.

5. Aktuator Termal mengubah energi listrik menjadi perubahan suhu untuk pemanasan atau pendinginan.

Contoh: Elemen pemanas dalam setrika listrik atau pendingin termoelektrik *Peltier* dalam sistem pengatur suhu.

6. Aktuator Digital bertindak dalam ranah perangkat lunak untuk menjalankan aksi berbasis sistem elektronik.

Contoh: Pengiriman email otomatis, peringatan notifikasi, atau sistem alarm berbasis IoT.

Beberapa contoh aplikasi penggunaan dari aktuator, diantaranya:

- Otomasi Rumah dalam mengontrol kipas, lampu pintar, gorden otomatis, dan pintu garasi otomatis.
- Industri & Manufaktur dalam mengoperasikan mesin otomatis, sistem perakitan robotik, dan *conveyor*.
- Otomotif dalam mengontrol suspensi adaptif, rem otomatis, dan sistem kemudi listrik.
- Medis & Kesehatan dalam menggerakkan alat bantu jalan otomatis, mengontrol pompa infus, atau mengatur ventilator medis.
- Keamanan & Militer dalam mengaktifkan sistem keamanan seperti kunci otomatis dan kamera pengawas yang dapat bergerak secara dinamis.

3.6 Unit Pemrosesan Data dalam IoT

Unit pemrosesan data berfungsi sebagai “otak” untuk mengolah data, menjalankan algoritma, dan mengendalikan perangkat berdasarkan input dari sensor. Unit pemrosesan ini menentukan bagaimana perangkat IoT merespons lingkungan dan berinteraksi dengan sistem lainnya.

3.6.1 Sistem Tertanam (*Embedded Systems*) & Mikrokontroler

Sistem ini dirancang khusus untuk menjalankan tugas-tugas spesifik dalam perangkat IoT dengan konsumsi daya rendah dan efisiensi tinggi. Mikrokontroler biasanya memiliki CPU, memori, dan antarmuka input/output dalam satu chip. Beberapa contoh diantaranya:

1. Mikrokontroler

Mikrokontroler adalah unit pemrosesan kecil yang terintegrasi dengan unit pemrosesan, memori, dan antarmuka *input/output* dalam satu *chip*. Mikrokontroler digunakan dalam berbagai aplikasi IoT untuk membaca sensor, mengontrol aktuator, dan memproses data secara *real-time*.

- Arduino (ATmega328) merupakan salah satu mikrokontroler yang paling populer, digunakan dalam berbagai proyek elektronik dan IoT karena kemudahan penggunaannya serta dukungan komunitas yang luas.
- ESP32 merupakan mikrokontroler dengan konektivitas *Wi-Fi* dan Bluetooth bawaan, sering digunakan dalam aplikasi IoT yang membutuhkan komunikasi nirkabel.
- STM32 merupakan mikrokontroler berbasis *ARM Cortex* yang menawarkan performa tinggi dan efisiensi daya, cocok untuk aplikasi industri dan sistem tertanam yang kompleks.

2. *Single-board Computers (SBC)*

Single-board Computers (SBC) adalah komputer mini yang memiliki semua komponen utama dalam satu papan sirkuit. SBC lebih kuat dibandingkan mikrokontroler karena memiliki sistem operasi dan mendukung berbagai aplikasi yang lebih kompleks.

- Raspberry Pi merupakan SBC yang populer karena kemampuannya dalam menjalankan sistem

operasi berbasis *Linux*, mendukung aplikasi IoT, AI, dan komputasi *edge*.

- BeagleBone merupakan SBC yang dirancang untuk aplikasi industri dan robotika, menawarkan fleksibilitas tinggi serta GPIO (*General-Purpose Input/Output*) yang luas untuk mengontrol berbagai perangkat eksternal.

SBC sering digunakan untuk aplikasi yang membutuhkan pemrosesan lebih berat dibandingkan mikrokontroler, seperti analisis data *real-time*, server IoT, dan sistem otomatisasi yang lebih kompleks.

3.6.2 Prosesor dan Perangkat Computing

Prosesor dan perangkat komputasi dalam IoT berfungsi untuk memproses data, menjalankan algoritma, dan mengontrol perangkat. Beberapa contoh diantaranya:

1. Prosesor untuk IoT dan AI

Beberapa sistem IoT yang membutuhkan kecerdasan buatan (AI) dan pemrosesan data besar menggunakan prosesor khusus yang dioptimalkan untuk pembelajaran mesin dan analisis data kompleks. Contohnya yaitu:

- Prosesor khusus IoT seperti *Qualcomm Snapdragon Wear*, *ARM Cortex-M*.
- Prosesor AI seperti *Sensor Processing Unit (TPU)* *Google*, *Edge TPU*, *Intel Neural Compute Stick*.

2. Perangkat Edge Computing

Unit pemrosesan yang memungkinkan komputasi dilakukan di dekat sumber data, mengurangi latensi, dan mengurangi ketergantungan pada server pusat (*cloud*) (Bittencourt *et al.*, 2018). Cocok untuk aplikasi *real-time* seperti visi komputer dan analisis data cepat. Contohnya yaitu *NVIDIA Jetson*, *Google Coral*, *Intel Movidius*.

3. *Cloud Computing* dan *Server Backend*

Untuk perangkat IoT dengan keterbatasan daya dan kapasitas pemrosesan, sebagian besar komputasi dilakukan di *cloud* (Sembroiz, Ricciardi and Careglio, 2017; Bittencourt *et al.*, 2018; Temucin *et al.*, 2018). Server ini mengelola data dalam jumlah besar, analitik cerdas, dan integrasi antarperangkat IoT. Sebagai contoh: *AWS IoT*, *Microsoft Azure IoT*, *Google Cloud IoT*.

3.6.3 Peran Unit Pemrosesan Data dalam IoT

Beberapa peran dan fungsi dari unit pemrosesan data dalam sistem IoT diantaranya, yaitu :

1. Pemrosesan Data

Unit pemrosesan berfungsi untuk mengolah data yang dikumpulkan dari sensor sebelum dikirim ke *cloud* atau perangkat lain. Proses ini mencakup penyaringan, pengolahan, dan penyusunan data agar dapat digunakan untuk analisis lebih lanjut.

2. Manajemen Perangkat

Selain mengolah data, unit pemrosesan juga bertanggung jawab dalam mengontrol aktuator, mengatur konektivitas, serta memastikan komunikasi yang optimal antarperangkat dalam sistem IoT.

3. Keamanan & Enkripsi

Untuk melindungi data dari akses yang tidak sah, unit pemrosesan menerapkan teknik enkripsi dan autentikasi. Ini penting dalam menjaga integritas dan kerahasiaan informasi yang dipertukarkan antarperangkat.

4. Analitik & AI

Dengan kemampuan analitik dan kecerdasan buatan (AI), unit pemrosesan dapat menganalisis data secara *real-time* dan mengambil keputusan cerdas secara otomatis. Hal ini memungkinkan sistem IoT bekerja

lebih efisien tanpa terlalu bergantung pada intervensi manusia.

DAFTAR PUSTAKA

- Adere, E.M. (2022) 'Blockchain in healthcare and IoT: A systematic literature review', *Array*, 14. Available at: <https://doi.org/10.1016/j.array.2022.100139>.
- Bittencourt, L. *et al.* (2018) 'The Internet of Things, Fog and Cloud continuum: Integration and challenges', *Internet of Things (Netherlands)*, 3–4, pp. 134–155. Available at: <https://doi.org/10.1016/j.iot.2018.09.005>.
- GeeksforGeeks (2020) *Understanding 'Things' in Internet of Things* - *GeeksforGeeks*. Available at: <https://www.geeksforgeeks.org/understanding-things-in-internet-of-things/> (Accessed: 2 March 2025).
- Gopal, S.B., Poongodi, C. and Nanthiya, D. (2022) 'Blockchain-based secured payment in IoE', *Smart Energy and Electric Power Systems: Current Trends and New Intelligent Perspectives*, pp. 185–200. Available at: <https://doi.org/10.1016/B978-0-323-91664-6.00009-7>.
- Inbamani, A. *et al.* (2022) 'Role of IoT and semantics in e-Health', *Semantic Models in IoT and eHealth Applications*, pp. 19–37. Available at: <https://doi.org/10.1016/B978-0-32-391773-5.00008-X>.
- Inui, T. *et al.* (2017) 'IoT Technologies: State of the Art and a Software Development Framework', *Smart Sensors Networks: Communication Technologies and Intelligent Applications*, pp. 3–18. Available at: <https://doi.org/10.1016/B978-0-12-809859-2.00002-4>.
- Kala, S. and Nalesh, S. (2022) 'Security and challenges in IoT-enabled systems', *System Assurances: Modeling and Management*, pp. 437–445. Available at: <https://doi.org/10.1016/B978-0-323-90240-3.00024-2>.
- Kiran, D.R. (2019) 'Internet of Things', *Production Planning and Control*, pp. 495–513. Available at: <https://doi.org/10.1016/B978-0-12-818364-9.00035-4>.

- Kraeling, M. and Brogioli, M.C. (2019) 'Internet of Things', *Software Engineering for Embedded Systems*, pp. 465–499. Available at: <https://doi.org/10.1016/B978-0-12-809448-8.00013-8>.
- Mathur, S. *et al.* (2023) 'A Survey on Role of Blockchain for IoT: Applications and Technical Aspects', *Computer Networks*, 227. Available at: <https://doi.org/10.1016/j.comnet.2023.109726>.
- Ogonji, M.M., Okeyo, G. and Wafula, J.M. (2020) 'A survey on privacy and security of Internet of Things', *Computer Science Review*, 38. Available at: <https://doi.org/10.1016/j.cosrev.2020.100312>.
- Panahi Rizi, M.H. and Hosseini Seno, S.A. (2022) 'A systematic review of technologies and solutions to improve security and privacy protection of citizens in the smart city', *Internet of Things (Netherlands)*, 20. Available at: <https://doi.org/10.1016/j.iot.2022.100584>.
- Qays, M.O. *et al.* (2023) 'Key communication technologies, applications, protocols and future guides for IoT-assisted smart grid systems: A review', *Energy Reports*, 9, pp. 2440–2452. Available at: <https://doi.org/10.1016/j.egyr.2023.01.085>.
- Sembroiz, D., Ricciardi, S. and Careglio, D. (2017) 'A Novel Cloud-Based IoT Architecture for Smart Building Automation', *Security and Resilience in Intelligent Data-Centric Systems and Communication Networks*, pp. 215–233. Available at: <https://doi.org/10.1016/B978-0-12-811373-8.00010-0>.
- Temucin, H. *et al.* (2018) 'A cloud-based big data system to support visually impaired people', *Computational Intelligence for Multimedia Big Data on the Cloud with Engineering Applications*, pp. 1–22. Available at: <https://doi.org/10.1016/B978-0-12-813314-9.00001-3>.
- Wolf, M. (2023) 'Embedded Computing', *Computers as Components*, pp. 1–52. Available at: <https://doi.org/10.1016/B978-0-323-85128-2.00001>.

BAB 4

PRINSIP KONEKSI PADA IoT

Oleh Muhammad Nuzan Rizki

4.1 Pendahuluan

Koneksi merupakan salah satu elemen utama dalam *Internet of Things* (IoT) yang memungkinkan perangkat untuk saling berkomunikasi, berbagi data, dan bekerja secara terpadu. Dalam ekosistem IoT, koneksi mencakup aliran informasi dari perangkat fisik seperti sensor dan aktuator, melalui jaringan komunikasi, hingga layanan *cloud* atau aplikasi pengguna akhir. Proses ini menjadi fondasi bagi berbagai aplikasi IoT, mulai dari pemantauan lingkungan hingga pengelolaan perangkat pintar di rumah.

Pada dasarnya, koneksi IoT melibatkan interaksi antara perangkat keras dan perangkat lunak melalui protokol komunikasi tertentu. Protokol ini dirancang untuk memastikan pengiriman data yang efisien, handal, dan aman. Selain itu, keberagaman teknologi koneksi seperti Wi-Fi, Bluetooth, LoRa, hingga 5G, memberikan fleksibilitas bagi pengembang dalam memilih solusi yang sesuai dengan kebutuhan aplikasi IoT mereka. Dalam konteks IoT, konektivitas mengacu pada kemampuan perangkat untuk terhubung dengan jaringan internet maupun dengan perangkat lainnya, sehingga data dapat dikumpulkan, dianalisis, dan digunakan untuk pengambilan keputusan yang lebih baik.

Proses koneksi dalam IoT melibatkan berbagai protokol dan teknologi komunikasi yang memungkinkan perangkat untuk saling bertukar informasi. Protokol seperti MQTT (Message

Queueing Telemetry Transport) dan CoAP (*Constrained Application Protocol*) dirancang khusus untuk lingkungan yang memiliki keterbatasan sumber daya, dan sangat efektif dalam aplikasi IoT (Nugroho, Setyawan and Zainuri, 2018; Seetaiah, 2023).

Bab ini akan membahas prinsip dasar koneksi IoT, mulai dari komponen yang terlibat, alur data yang terjadi, hingga teknologi dan protokol yang mendukung keberlangsungan komunikasi antarperangkat IoT. Pemahaman terhadap dasar-dasar ini sangat penting untuk mengembangkan solusi IoT yang andal, hemat energi, dan mampu beradaptasi dengan kebutuhan masa depan.

4.2 Dasar-Dasar Koneksi

Koneksi dalam konteks Internet of Things (IoT) mengacu pada kemampuan perangkat-perangkat yang terhubung untuk saling berkomunikasi dan bertukar data melalui jaringan internet (Gambar 4.1). Dalam ekosistem IoT, perangkat tersebut dapat mencakup sensor, aktuator, komputer, dan berbagai alat elektronik lainnya yang dilengkapi dengan kemampuan konektivitas. Koneksi ini memungkinkan perangkat untuk tidak hanya mengirim dan menerima data, tetapi juga berkolaborasi dalam melakukan tugas tertentu, memproses informasi, dan mengambil keputusan berdasarkan data yang dikumpulkan (Kodati *et al.*, 2021; Prakash *et al.*, 2022).



Gambar 4. 1 Kemampuan Konektifitas Antar Perangkat dalam Ekosistem IoT

Pada dasarnya, koneksi IoT dapat terbagi menjadi beberapa lapisan, termasuk:

- ✓ Lapisan Akses. Merupakan area di mana perangkat IoT melakukan koneksi ke jaringan. Ini dapat meliputi konektor seperti Wi-Fi, Bluetooth, Zigbee, atau teknologi nirkabel lainnya yang memungkinkan perangkat untuk terhubung ke internet atau ke perangkat lain dalam jaringan lokal.
- ✓ Lapisan Jaringan. Setelah perangkat terhubung, data harus dikirim melalui jaringan. Ini mencakup penggunaan protokol transmisi data seperti MQTT atau CoAP yang memastikan data dapat dikirim dengan efisien antara perangkat dan aplikasi.
- ✓ Lapisan Aplikasi. Di sini, data yang telah dikumpulkan diproses dan dianalisis. Aplikasi IoT yang beroperasi di lapisan ini memungkinkan pengguna untuk memvisualisasikan data, mengelola perangkat, dan melakukan interaksi dengan hasil yang diperoleh dari koneksi IoT.

Konektivitas ini bukan hanya memfasilitasi transfer data, tetapi juga memungkinkan pengumpulan informasi dalam *real-time*, sehingga meningkatkan kemampuan analisis dan respons terhadap kondisi yang berubah. Dengan adanya koneksi yang

tepat dan aman, perangkat IoT dapat berfungsi secara optimal, membuka berbagai aplikasi termasuk otomatisasi rumah, pemantauan kesehatan jarak jauh, dan pengelolaan sumber daya yang lebih efisien.

4.3 Protokol Koneksi IoT

Di dalam dunia Internet of Things (IoT), protokol koneksi memainkan peran yang sangat penting dalam memfasilitasi komunikasi antara perangkat, serta menjamin bahwa data dapat dikirim dan diterima secara efisien dan andal. Protokol ini adalah sekumpulan aturan dan standar yang mendefinisikan cara perangkat terhubung dan berinteraksi dalam jaringan. Berikut adalah beberapa protokol koneksi IoT yang paling umum digunakan.

- *Message Queuing Telemetry Transport (MQTT)*
Salah satu protokol yang paling banyak digunakan adalah MQTT. Protokol ini dirancang untuk komunikasi yang ringan dan efisien, ideal untuk aplikasi dengan *bandwidth* rendah dan keterbatasan sumber daya. MQTT menggunakan model *publish/subscribe*, memungkinkan perangkat untuk mengirim data (*publish*) dan menerima data dari topik tertentu (*subscribe*) tanpa perlu langsung terhubung satu sama lain. Hal ini membuatnya sangat efisien untuk aplikasi IoT yang memerlukan pengiriman data secara real-time (Giambona, Redondi and Cesana, 2018; Akshatha, Kumar and R, 2022).
- *Constrained Application Protocol (CoAP)*
CoAP adalah protokol lain yang dirancang khusus untuk perangkat IoT dengan keterbatasan sumber daya. CoAP beroperasi pada prinsip yang mirip dengan HTTP, tetapi dioptimalkan untuk latensi rendah dan efisiensi jaringan. Protokol ini mendukung komunikasi dalam mode *request-response* dan sangat baik untuk komunikasi M2M (*Machine*

to Machine) di lingkungan yang memiliki perangkat sensor yang lebih sederhana (Spina and De Rango, 2023).

- HTTP/HTTPS

HTTP/HTTPS juga digunakan dalam aplikasi IoT, terutama untuk aplikasi yang memerlukan interaksi dengan web. Meski memiliki overhead yang lebih tinggi dibandingkan MQTT dan CoAP, HTTPS menawarkan enkripsi yang kuat dan keamanan tambahan saat mentransfer data sensitif, sehingga cocok untuk aplikasi IoT yang memerlukan perlindungan privasi.

- *WebSocket*

WebSocket menjadi populer dalam aplikasi IoT yang membutuhkan komunikasi dua arah real-time. Protokol ini memungkinkan koneksi terus menerus antara klien dan server, sehingga data dapat dikirim secara langsung tanpa perlu mengirim permintaan baru setiap kali. Ini sangat cocok untuk aplikasi yang memerlukan pembaruan berkala, seperti pemantauan kesehatan atau otomasi rumah.

- *Long Range Wide Area Network (LoRaWAN)* dan *SigFox*

Selain itu, protokol seperti LoRaWAN dan SigFox dirancang untuk komunikasi jarak jauh dengan konsumsi daya rendah. LoRaWAN memungkinkan perangkat untuk beroperasi dalam jaringan yang luas dengan kebutuhan daya minimum, sedangkan SigFox menggunakan frekuensi radio untuk menghubungkan perangkat IoT secara efisien dalam region yang lebih besar tanpa memerlukan infrastruktur jaringan kompleks. Akhirnya, penting untuk mempertimbangkan aspek keamanan dalam protokol koneksi IoT. Protokol seperti DTLS (*Datagram Transport Layer Security*) dan TLS (*Transport Layer Security*) digunakan untuk mengenkripsi data dan memastikan bahwa komunikasi antar perangkat terlindungi dari ancaman luar. Dengan mengintegrasikan aspek keamanan dalam protokol koneksi, perkembangan solusi IoT dapat dilakukan dengan lebih aman dan terpercaya.

Secara keseluruhan, pemilihan protokol koneksi yang tepat sangat penting untuk memastikan komunikasi yang efektif, efisien, dan aman dalam aplikasi IoT. Protokol yang berbeda memiliki keunggulan dan kekurangan masing-masing, dan keputusan untuk menggunakan salah satu dari mereka harus didasarkan pada kebutuhan spesifik aplikasi yang sedang dikembangkan.

4.4 Teknologi Koneksi IoT

Teknologi koneksi dalam *Internet of Things* (IoT) mencakup berbagai metode, perangkat, dan infrastruktur yang memungkinkan komunikasi antara perangkat yang terhubung. Dengan semakin berkembangnya IoT, berbagai teknologi koneksi muncul untuk memenuhi kebutuhan spesifik dari aplikasi yang berbeda. Dalam subbab ini, kita akan membahas beberapa teknologi koneksi IoT yang paling umum digunakan.

Pertama-tama, **Wi-Fi** adalah salah satu teknologi koneksi yang paling luas digunakan untuk perangkat IoT. Dengan kecepatan tinggi dan kapasitas transfer data yang besar, Wi-Fi sangat cocok untuk aplikasi yang memerlukan koneksi berkelanjutan dan *bandwidth* tinggi, seperti kamera keamanan dan perangkat pintar di rumah. Namun, Wi-Fi memerlukan akses ke sumber daya listrik dan jaringan lokal, yang dapat menjadi pembatas dalam aplikasi yang berkembang di lokasi terpencil.



Gambar 4. 2 Ilustrasi Penggunaan Teknologi Wi-fi dalam Komunikasi Antar Perangkat IoT

Teknologi Wi-Fi telah menjadi salah satu standar komunikasi nirkabel yang paling umum digunakan untuk menghubungkan perangkat *Internet of Things* (IoT). Ketersediaannya yang luas dan fitur robust menawarkan berbagai kelebihan untuk aplikasi IoT. Berikut adalah beberapa kelebihan utama dari penggunaan Wi-Fi untuk perangkat IoT (Hariram *et al.*, 2021; Abderrahmane, Nourredine and Mohammed, 2024).

Salah satu manfaat utama dari Wi-Fi adalah kecepatan transfer data yang tinggi. Dibandingkan dengan teknologi nirkabel lainnya seperti Zigbee atau LoRa, Wi-Fi dapat memberikan kecepatan yang jauh lebih tinggi, yang sangat penting untuk aplikasi yang memerlukan pengiriman data dalam jumlah besar dengan cepat. Kecepatan tinggi ini sangat bermanfaat untuk perangkat yang menangani streaming video, gambar berkualitas tinggi, atau tugas pemrosesan data yang signifikan, sehingga meningkatkan pengalaman pengguna dan fungsionalitas.

Selain itu, cakupan area yang luas yang dapat disediakan oleh Wi-Fi juga merupakan keuntungan besar. Dengan adanya kemajuan dalam standar Wi-Fi, seperti Wi-Fi 6, cakupan jaringan telah meningkat, memungkinkan lebih banyak perangkat untuk terhubung secara efektif di jarak yang lebih jauh. Kemampuan

ini sangat penting untuk rumah dan bangunan pintar, di mana banyak perangkat IoT perlu berkomunikasi dengan pusat kontrol atau layanan cloud tanpa kehilangan konektivitas.

Kemudahan integrasi juga merupakan keuntungan signifikan dari teknologi Wi-Fi. Jaringan Wi-Fi sudah umum di banyak lingkungan, dan sebagian besar perangkat IoT baru dilengkapi dengan kemampuan Wi-Fi bawaan. Kompatibilitas ini memungkinkan integrasi yang mulus ke dalam infrastruktur yang sudah ada tanpa memerlukan perangkat keras tambahan atau peralatan khusus. Akibatnya, ini mengarah pada biaya pemasangan yang lebih rendah dan proses instalasi yang lebih sederhana.

Interoperabilitas juga merupakan poin kuat Wi-Fi dalam IoT. Wi-Fi menggunakan protokol jaringan standar seperti TCP/IP, yang membuatnya lebih mudah bagi perangkat dari berbagai produsen untuk saling berkomunikasi. Fleksibilitas ini mendukung berbagai jenis aplikasi, mulai dari otomasi rumah hingga pemantauan industri, semuanya dalam satu jaringan yang terintegrasi.

Dalam hal keamanan, jaringan Wi-Fi dapat menerapkan protokol enkripsi lanjutan seperti WPA3, yang secara signifikan meningkatkan keamanan data yang dikirimkan melalui jaringan. Kemampuan untuk memanfaatkan langkah-langkah keamanan ini membantu melindungi informasi sensitif dari akses yang tidak sah, menjadi pertimbangan penting bagi perangkat IoT yang beroperasi di berbagai sektor, termasuk kesehatan dan keuangan.

Akhirnya, teknologi Wi-Fi terus berkembang dengan pengenalan kemampuan jaringan mesh. Jaringan mesh meningkatkan konektivitas dengan memungkinkan banyak perangkat untuk meneruskan data satu sama lain, memperluas cakupan dan keandalan di lingkungan di mana router tradisional mungkin kesulitan. Fitur ini menjadikan Wi-Fi sangat cocok untuk penerapan perangkat IoT yang padat di lingkungan seperti kota pintar atau pengaturan industri.

Secara keseluruhan, kelebihan menggunakan Wi-Fi untuk perangkat IoT mencakup kecepatan transfer data yang tinggi, cakupan luas, kemudahan integrasi, interoperabilitas, keamanan yang ditingkatkan, mobilitas, dan manfaat dari jaringan mesh. Fitur-fitur ini menjadikan Wi-Fi pilihan yang menarik untuk berbagai aplikasi IoT, mendukung permintaan yang terus berkembang untuk konektivitas yang handal dan efisien.

Kedua, **Zigbee** merupakan teknologi nirkabel yang dirancang untuk komunikasi jarak dekat dengan konsumsi daya rendah. Teknologi ini banyak digunakan di dalam Internet of Things (IoT), terutama pada aplikasi yang memerlukan konektivitas antara perangkat dengan daya rendah dan jarak komunikasi pendek. Zigbee biasa digunakan dalam aplikasi otomasi rumah, seperti sistem pencahayaan dan pengontrol suhu. Dengan kemampuan untuk menghubungkan hingga ratusan perangkat dalam jangkauan yang saling berdekatan, teknologi ini sangat efektif dalam membangun jaringan yang dapat diandalkan dengan biaya yang rendah.

Kelebihan Zigbee; Jangkauan Jaringan yang Luas. Dengan kemampuan jaringan mesh, Zigbee memungkinkan komunikasi antara perangkat pada jarak yang lebih jauh, sehingga sangat berguna untuk instalasi di area yang luas seperti di gedung komersial atau rumah pintar. Interoperabilitas: Zigbee dirancang untuk mendukung berbagai aplikasi dan perangkat dari berbagai produsen. Dengan adanya standarisasi, perangkat Zigbee umumnya dapat saling berkomunikasi meskipun berasal dari pabrikan yang berbeda. Keamanan: Zigbee dilengkapi dengan fitur keamanan yang mencakup enkripsi data dan autentikasi, sehingga membantu melindungi informasi yang dikirimkan dalam jaringan. Biaya Rendah: Biaya perangkat Zigbee umumnya rendah, dan biaya pemasangan jaringan juga ekonomis, menjadikannya solusi yang menarik bagi aplikasi skala besar seperti otomasi rumah dan pengendalian industri.

Selanjutnya, **LoRa (Long Range)** adalah teknologi yang dikembangkan untuk aplikasi IoT yang memerlukan cakupan daerah luas dengan konsumsi daya yang sangat rendah. LoRa memungkinkan perangkat untuk berkomunikasi jarak jauh, hingga beberapa kilometer, tanpa memerlukan infrastruktur jaringan seluler yang mahal. Teknologi ini ideal untuk aplikasi pemantauan lingkungan dan kota pintar, di mana banyak sensor harus tersebar di area yang luas.

NB-IoT (Narrowband IoT) adalah teknologi yang menggunakan jaringan seluler untuk menghubungkan perangkat IoT. Berbeda dengan teknologi 4G LTE, NB-IoT menawarkan efisiensi energi yang lebih baik dan penetrasi sinyal yang kuat di area tertutup, sehingga sangat cocok untuk aplikasi yang memerlukan konektivitas di dalam gedung, seperti perangkat kesehatan yang dipasang di rumah.

Selain itu, **Bluetooth Low Energy (BLE)** adalah teknologi yang dirancang untuk komunikasi jarak dekat dengan konsumsi daya yang rendah. BLE banyak digunakan dalam aplikasi seperti pelacakan kesehatan dan *wearable devices*, di mana perangkat perlu terhubung secara berkala tapi tidak memerlukan *bandwidth* tinggi. Teknologi ini memungkinkan perangkat untuk beroperasi selama sehari-hari atau bahkan berminggu-minggu dengan satu kali pengisian daya.

Teknologi koneksi lain yang semakin populer adalah 5G, yang menawarkan kecepatan transfer data yang sangat tinggi dan latensi yang rendah. Dengan kemampuan untuk menghubungkan jutaan perangkat secara simultan, 5G menjadi tulang punggung bagi banyak aplikasi IoT yang membutuhkan *bandwidth* tinggi, seperti kendaraan otonom dan aplikasi real-time lainnya. Teknologi ini juga memungkinkan penggunaan *edge computing*, di mana data dapat diproses secara lokal untuk meningkatkan respons dan efisiensi.

Akhirnya, teknologi satelit juga mulai diterapkan dalam IoT, terutama untuk aplikasi yang tidak dapat dijangkau oleh jaringan seluler atau Wi-Fi. Misalnya, dalam sektor

pertambangan atau pemantauan laut. Teknologi ini memungkinkan komunikasi dengan perangkat yang terletak di lokasi remote, memberikan solusi koneksi yang komprehensif untuk aplikasi IoT global.

Secara keseluruhan, teknologi koneksi IoT terus berkembang untuk memenuhi kebutuhan yang bervariasi dari berbagai aplikasi. Pemilihan teknologi yang tepat sangat penting untuk memastikan efisiensi, keamanan, dan keberhasilan sistem IoT yang sedang dikembangkan.

DAFTAR PUSTAKA

- Abderrahmane, T., Nourredine, A. and Mohammed, T. (2024) 'Experimental analysis for comparison of wireless transmission technologies: Wi-Fi, Bluetooth, ZigBee and LoRa for mobile multi-robot in hostile sites', *International Journal of Electrical and Computer Engineering (IJECE)* [Preprint]. Available at: <https://api.semanticscholar.org/CorpusID:268941878>.
- Akshatha, P.S., Kumar, S.M.D. and R, V.K. (2022) 'MQTT Implementations, Open Issues, and Challenges: A Detailed Comparison and Survey', *International Journal of Sensors, Wireless Communications and Control* [Preprint]. Available at: <https://api.semanticscholar.org/CorpusID:254919554>.
- Seetaiah, B. (2023) 'Enhancing Device Provisioning and Connectivity in IoT Systems Using Azure IoT Hub and DPS: A Case Study', *International Journal of Scientific Research and Engineering Trends* [Preprint]. Available at: <https://api.semanticscholar.org/CorpusID:273137063>.
- Giambona, R., Redondi, A.E.C. and Cesana, M. (2018) 'MQTT+: Enhanced Syntax and Broker Functionalities for Data Filtering, Processing and Aggregation', *ArXiv*, abs/1810.00773. Available at: <https://api.semanticscholar.org/CorpusID:52898564>.
- Hariram, M. *et al.* (2021) 'Performance Analysis of Wi-Fi and LoRa Technology and its Implementation in Farm Monitoring System', *IOP Conference Series: Materials Science and Engineering*, 1055. Available at: <https://api.semanticscholar.org/CorpusID:234089670>.
- Kodati, S. *et al.* (2021) 'Security Framework Connection Assistance for IoT Device Secure Data communication', *E3S Web of Conferences* [Preprint]. Available at: <https://api.semanticscholar.org/CorpusID:241541805>.

- Nugroho, R.W., Setyawan, R.A. and Zainuri, A. (2018) 'Sistem Monitoring Curah Hujan Berbasis Internet Of Things (Iot) Menggunakan Tipping Bucket Terintegrasi Aplikasi Pada Smartphone', in. Available at: <https://api.semanticscholar.org/CorpusID:86530242>.
- Prakash, P. *et al.* (2022) 'IoT Device Friendly and Communication-Efficient Federated Learning via Joint Model Pruning and Quantization', *IEEE Internet of Things Journal*, 9(15), pp. 13638–13650. Available at: <https://doi.org/10.1109/JIOT.2022.3145865>.
- Spina, M.G. and De Rango, F. (2023) 'Lightweight, Dynamic and Energy Efficient Security Mechanism for constrained IoT devices using CoAP', in *2023 IEEE 20th Consumer Communications & Networking Conference (CCNC)*. IEEE, pp. 1123–1128. Available at: <https://doi.org/10.1109/CCNC51644.2023.10059854>.

BAB 5

IP SEBAGAI LAPISAN JARINGAN PADA IoT

Oleh Ali Impron

5.1 Pendahuluan

Internet of Things (IoT) merupakan jaringan yang terhubung secara global, menghubungkan perangkat fisik dengan kemampuan untuk mengumpulkan dan bertukar data tanpa intervensi manusia (Abood *et al.*, 2024; Kayyali, 2022; Verma *et al.*, 2022). Dalam hal ini, *Internet Protocol* (IP) menjadi lapisan jaringan utama, karena IP menyediakan mekanisme yang memungkinkan perangkat IoT untuk berkomunikasi dan beroperasi di lingkungan yang saling terhubung. Sebagai teknologi dasar yang memungkinkan perangkat untuk mengakses dan mengirim data dalam jaringan, IP menghadirkan fondasi yang stabil dan terstandarisasi bagi komunikasi di antara perangkat IoT yang tersebar secara luas (Mali and Nimkar, 2017; Patel *et al.*, 2021; Sivaraman *et al.*, 2018).

IP, sebagai protokol standar dalam jaringan internet, memastikan bahwa setiap perangkat IoT dapat terhubung dengan unik melalui pengalamatan khusus yang dimiliki masing-masing perangkat. Dalam jaringan IoT, di mana miliaran perangkat terhubung, IP memberikan solusi skala besar yang mampu mengatasi kebutuhan pengalamatan. Pengalamatan unik ini memungkinkan identifikasi dan interaksi antar perangkat dalam aplikasi IoT yang melibatkan pemantauan dan pengendalian jarak jauh, baik dalam konteks rumah pintar, kota cerdas, maupun industri.

Dalam dekade terakhir, peningkatan eksponensial jumlah perangkat yang terhubung ke internet menuntut penggunaan alamat IP yang lebih efisien. IPv4, protokol IP generasi awal, memiliki tantangan keterbatasan alamat yang hanya memiliki ruang pengalamatan sekitar 4,3 miliar alamat. Sementara itu, IPv6 muncul sebagai solusi yang menawarkan kapasitas pengalamatan yang jauh lebih besar, yaitu sekitar $3,4 \times 10^{38}$ alamat, untuk mengakomodasi ledakan perangkat IoT yang tidak terbatas.

Standarisasi IP dalam IoT tidak hanya menyediakan pengalamatan tetapi juga memastikan kompatibilitas antar perangkat yang diproduksi oleh berbagai vendor. Dalam jaringan IoT yang heterogen, di mana perangkat dari berbagai jenis dan kapasitas terlibat, IP memungkinkan komunikasi yang konsisten dan aman melalui protokol lapisan jaringan. Misalnya, komunikasi antar perangkat rumah pintar dengan sensor lingkungan atau perangkat dalam sistem transportasi cerdas dapat dilakukan dengan lancar berkat standar yang diberikan oleh IP.

Selain itu, keberadaan IP memungkinkan protokol-protokol lapisan aplikasi yang umum dalam IoT seperti CoAP, MQTT, dan HTTP untuk berjalan pada infrastruktur yang sama. Dengan menggunakan IP sebagai lapisan jaringan, IoT dapat memanfaatkan infrastruktur internet yang telah ada, sehingga mengurangi biaya implementasi dan memudahkan pengembangan lebih lanjut. Hal ini memberikan keuntungan besar bagi industri, karena mereka dapat memanfaatkan arsitektur yang ada untuk mempercepat penerapan IoT dalam berbagai aplikasi.

5.2 Konsep Dasar Internet Protocol (IP) dalam IoT

Internet Protocol (IP) adalah protokol komunikasi utama yang digunakan di dalam internet dan jaringan komputer (Giambene, 2021; Tian and Gao, 2024), bertanggung jawab untuk mengarahkan paket data dari satu titik ke titik lain dalam jaringan. Dalam konteks *Internet of Things* (IoT), IP memainkan peran krusial, memungkinkan setiap perangkat IoT mendapatkan alamat unik yang memungkinkan mereka untuk saling terhubung dan berkomunikasi secara langsung melalui jaringan. Dengan menggunakan pengalamatan IP, setiap perangkat IoT dapat dikenali secara spesifik, memungkinkan pengiriman data secara tepat antara perangkat pengirim dan penerima.

IP dirancang untuk menjadi protokol yang mampu mengakomodasi jaringan yang sangat luas, termasuk IoT. Dalam jaringan ini, IP menyediakan fungsi-fungsi utama seperti:

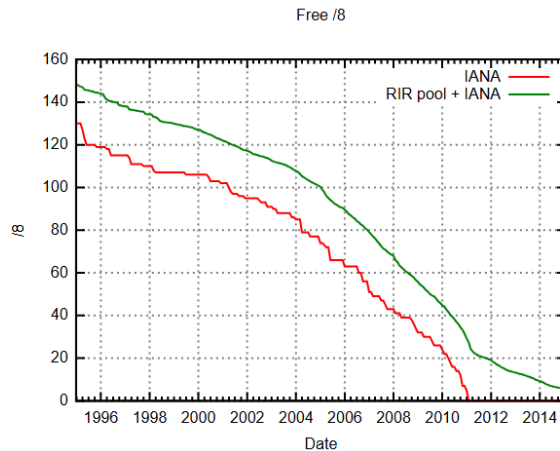
- ✓ **Pengalamatan (*Addressing*):** Setiap perangkat IoT membutuhkan alamat unik untuk identifikasi, sehingga memungkinkan komunikasi langsung dengan perangkat lain.
- ✓ **Fragmentasi dan *Reassembly*:** Paket data besar dapat dipecah menjadi fragmen yang lebih kecil agar sesuai dengan batasan ukuran paket dalam jaringan IoT dan kemudian disusun kembali pada penerima.
- ✓ ***Routing*:** Fungsi ini memastikan paket data mencapai tujuan yang diinginkan dengan melewati berbagai node atau perangkat perantara di jaringan.

Sebagai dasar dalam jaringan IoT, IP memiliki fungsi tambahan untuk memungkinkan mobilitas perangkat, mengingat banyak perangkat IoT beroperasi secara nirkabel dan bergerak, misalnya, pada aplikasi seperti pelacakan aset dan sistem transportasi pintar.

Sejak awal penggunaannya, IPv4 adalah versi IP yang umum diterapkan dalam jaringan internet. Namun, seiring

meningkatnya jumlah perangkat yang terhubung, batasan kapasitas IPv4 menjadi kendala tersendiri. IPv4 hanya memiliki ruang pengalamatan sebesar 32-bit, yang mampu mendukung sekitar 4,3 miliar alamat unik. Dengan jumlah perangkat IoT yang diperkirakan mencapai puluhan miliar dalam waktu dekat, kapasitas ini tidak lagi mencukupi.

Sebagai jawaban atas keterbatasan tersebut, IPv6 diperkenalkan sebagai standar baru dengan ruang pengalamatan 128-bit yang memungkinkan sekitar $3,4 \times 10^{38}$ alamat unik. Keunggulan ini membuat IPv6 sangat cocok untuk jaringan IoT yang besar dan kompleks, di mana setiap perangkat, mulai dari sensor terkecil hingga sistem besar, memerlukan pengalamatan individu. Selain kapasitas pengalamatan yang lebih besar, IPv6 juga menawarkan fitur-fitur tambahan seperti autokonfigurasi dan dukungan untuk mobilitas, yang sangat dibutuhkan dalam ekosistem IoT.



Gambar 5. 1 Grafik Kehabisan Alamat IPv4
(Sumber : www.iana.org)

5.3 Perbedaan IPv4 dan IPv6 pada IoT

Perkembangan jaringan Internet of Things (IoT) menuntut jaringan IP yang fleksibel dan mampu mengakomodasi sejumlah besar perangkat. Meski IPv4 telah menjadi standar utama dalam

komunikasi jaringan selama beberapa dekade, pertumbuhan IoT menghadirkan tantangan baru yang membuat IPv6 menjadi pilihan lebih tepat. Pada halaman ini, kita akan mengeksplorasi perbedaan antara IPv4 dan IPv6, serta kesesuaian keduanya dalam mendukung kebutuhan IoT.

Perbedaan mendasar antara IPv4 dan IPv6 terletak pada panjang dan kapasitas ruang pengalamatan. IPv4 menggunakan alamat 32-bit yang menghasilkan sekitar 4,3 miliar alamat unik. Walaupun ini cukup untuk internet pada era awal, lonjakan perangkat yang terhubung ke jaringan, khususnya perangkat IoT, membuat jumlah ini menjadi tidak memadai. Sebaliknya, IPv6 menggunakan alamat 128-bit yang memungkinkan total ruang pengalamatan hingga $3,4 \times 10^{38}$, cukup untuk mengakomodasi jumlah perangkat IoT yang terus meningkat di masa mendatang.

Skalabilitas yang disediakan IPv6 memberi keleluasaan bagi pengembang IoT untuk merancang jaringan tanpa takut kehabisan alamat IP. Selain itu, IPv6 memungkinkan penggunaan pengalamatan hirarkis yang lebih efisien, mempermudah pengaturan jaringan yang kompleks, serta mendukung aplikasi IoT di berbagai sektor seperti manufaktur, transportasi, dan industri.

Selain kemampuan skalabilitasnya, IPv6 memiliki beberapa keunggulan tambahan yang membuatnya lebih cocok untuk IoT, yaitu:

1. Autokonfigurasi: IPv6 memiliki kemampuan autokonfigurasi melalui fitur Stateless Address Autoconfiguration (SLAAC), yang memungkinkan perangkat mendapatkan alamat IP secara otomatis saat terhubung ke jaringan. Hal ini sangat bermanfaat dalam jaringan IoT yang terdiri dari jutaan perangkat yang mungkin tidak memiliki akses langsung untuk konfigurasi manual.
2. Kualitas Layanan (QoS) yang Lebih Baik: IPv6 mendukung prioritas data dengan memberikan dukungan untuk kualitas layanan (QoS). Fitur ini bermanfaat terutama untuk aplikasi

yang memerlukan respons real-time, seperti pemantauan kesehatan atau transportasi cerdas, di mana data prioritas tinggi harus diproses lebih cepat.

3. Keamanan Terintegrasi: IPv6 dirancang dengan dukungan untuk IPsec (*Internet Protocol Security*) sebagai bagian dari standar. IPsec menyediakan fitur enkripsi dan otentikasi yang lebih kuat, untuk menjaga keamanan data pada jaringan IoT, terutama yang berisiko tinggi terhadap akses tidak sah atau serangan siber.
4. Routing yang Lebih Efisien: Struktur alamat IPv6 memungkinkan routing yang lebih efisien di jaringan besar. Dengan dukungan pengalamatan *multicast*, IPv6 memfasilitasi pengiriman data ke beberapa perangkat sekaligus tanpa harus membuat beberapa salinan paket, mengurangi beban lalu lintas jaringan, serta menghemat *bandwidth*. Ini memberikan efisiensi besar dalam pengiriman data IoT, terutama pada jaringan dengan jumlah node yang banyak.

Walaupun IPv6 memiliki keunggulan signifikan, transisi dari IPv4 ke IPv6 di lingkungan IoT masih menghadapi beberapa tantangan. Salah satu hambatan utama adalah keberadaan infrastruktur berbasis IPv4 yang telah mapan, terutama di lingkungan industri yang sudah mengadopsi IoT dengan perangkat IPv4. Peningkatan perangkat keras atau lunak untuk mendukung IPv6 sering kali memerlukan biaya tambahan yang signifikan, yang menjadi tantangan bagi perusahaan atau organisasi yang tidak ingin mengganggu jaringan yang sudah berfungsi.

Selain itu, keterbatasan perangkat yang tidak mendukung IPv6 juga menjadi kendala. Banyak perangkat IoT yang lebih lama dirancang hanya untuk IPv4, sehingga tidak dapat diubah untuk mendukung IPv6 tanpa *upgrade*. Untuk mengatasi kendala ini, beberapa pendekatan digunakan, seperti penggunaan gateway yang mampu mengonversi lalu lintas IPv6 ke IPv4, atau

dengan menggunakan mekanisme dual-stack yang memungkinkan jaringan untuk mendukung keduanya.

Dalam beberapa implementasi IoT, solusi hybrid seperti dual-stack dan NAT64/DNS64 digunakan untuk mendukung komunikasi antara IPv4 dan IPv6. Pendekatan dual-stack memungkinkan perangkat IoT beroperasi dengan kedua versi IP secara bersamaan, sehingga perangkat IPv4 tetap dapat berkomunikasi dalam jaringan yang sebagian besar telah menggunakan IPv6. Sementara itu, NAT64/DNS64 memungkinkan perangkat berbasis IPv6 untuk berkomunikasi dengan perangkat IPv4 dengan menerjemahkan alamat IPv6 menjadi IPv4.

Implementasi solusi *hybrid* ini memberikan fleksibilitas bagi jaringan IoT yang memiliki perangkat campuran, serta menjadi strategi transisi yang efektif untuk mengakomodasi pertumbuhan IoT tanpa harus memperbarui seluruh infrastruktur ke IPv6 secara langsung.

5.4 Pengelolaan Alamat IP dalam Jaringan IoT

Dalam jaringan IoT, pengelolaan alamat IP adalah elemen kritis yang memastikan perangkat dapat terhubung dan berkomunikasi secara efisien. Karena jaringan IoT sering kali melibatkan ribuan hingga jutaan perangkat, pengaturan alamat IP menjadi tugas yang kompleks dan membutuhkan pendekatan yang efisien serta adaptif. Pada bab ini, kita akan membahas metode alokasi alamat, pengelolaan alamat dinamis dan statis, serta peran *Domain Name System* (DNS) dalam jaringan IoT.

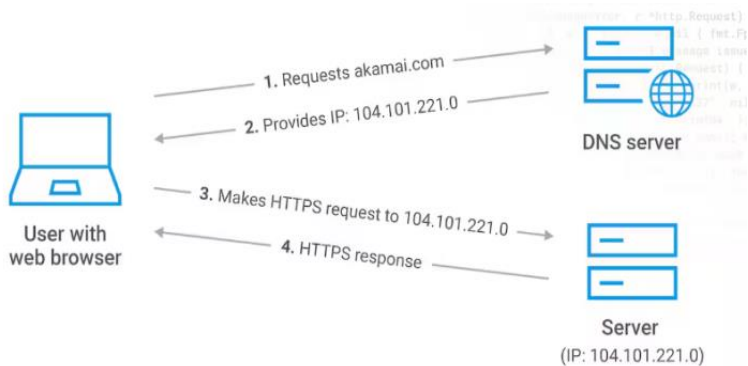
Sistem Alokasi Alamat IP pada Jaringan IoT

Alokasi alamat IP pada jaringan IoT dapat dilakukan dengan beberapa pendekatan tergantung pada jenis perangkat, kebutuhan jaringan, dan kompleksitas topologi. Dua metode utama alokasi IP pada IoT adalah alokasi dinamis dan statis:

1. **Alamat IP Statis:** Alamat IP statis diberikan secara manual dan tetap untuk setiap perangkat dalam jaringan. Alokasi ini umum diterapkan pada perangkat IoT yang kritis dan memiliki fungsi khusus yang membutuhkan identifikasi tetap. Penggunaan alamat statis memudahkan dalam pengelolaan perangkat utama seperti *gateway* atau *server*, karena alamatnya tidak berubah. Namun, metode ini menjadi tidak praktis untuk jumlah perangkat yang sangat besar, seperti pada aplikasi IoT skala besar, karena pengaturan dan pemeliharaan alamat statis untuk setiap perangkat bisa sangat memakan waktu.
2. **Alamat IP Dinamis:** Dalam jaringan IoT yang besar dan berskala luas, *Dynamic Host Configuration Protocol* (DHCP) sering digunakan untuk mengalokasikan alamat IP secara dinamis. Dengan DHCP, perangkat IoT dapat memperoleh alamat IP secara otomatis saat terhubung ke jaringan, tanpa memerlukan konfigurasi manual. Pendekatan ini memungkinkan efisiensi yang lebih tinggi dan fleksibilitas dalam mengelola perangkat yang mungkin sering berganti atau tidak selalu terhubung ke jaringan. DHCP adalah solusi yang umum diterapkan pada perangkat IoT bergerak atau sementara, di mana koneksi dan alamat IP perlu diperbarui secara berkala.

Penggunaan DNS dalam Jaringan IoT

Domain Name System (DNS) memainkan peran penting dalam jaringan IoT karena memudahkan identifikasi perangkat melalui nama domain yang lebih mudah diingat daripada alamat IP numerik. DNS mengonversi nama domain yang ramah manusia (misalnya, *sensor.temperature.local*) menjadi alamat IP yang dapat dimengerti oleh jaringan. Penggunaan DNS sangat bermanfaat dalam jaringan IoT yang memiliki perangkat dengan alamat IP dinamis, sehingga perangkat tetap dapat diakses melalui nama domain mereka meskipun alamat IP-nya berubah.



Gambar 5. 2 Cara Kerja DNS

(Sumber : www.akamai.com)

Selain itu, penggunaan DNS di jaringan IoT mendukung pengelolaan perangkat dalam topologi yang lebih kompleks dan tersebar. DNS memungkinkan administrator jaringan mengelompokkan perangkat berdasarkan fungsi, lokasi, atau jenis perangkat, sehingga mempercepat pencarian dan identifikasi perangkat. Dalam beberapa kasus, DNS yang disesuaikan (mDNS atau *multicast* DNS) digunakan dalam IoT untuk mendukung lingkungan lokal atau jaringan tertutup, di mana perangkat IoT saling berkomunikasi tanpa membutuhkan koneksi internet.

Pengelolaan Alamat IP Berbasis Hierarki untuk Efisiensi

Dalam jaringan IoT berskala besar, pendekatan hierarkis dalam pengelolaan alamat IP sering kali diimplementasikan untuk menjaga efisiensi dan mengurangi beban routing. Pengelolaan hierarki ini memungkinkan administrator jaringan untuk mengelompokkan perangkat IoT berdasarkan lokasi geografis, jenis layanan, atau tingkat kepentingan. Sebagai contoh, dalam jaringan IoT untuk kota cerdas, perangkat sensor lalu lintas di wilayah tertentu dapat dikelompokkan dalam sub-jaringan dengan rentang IP khusus yang berbeda dari sub-jaringan sensor lingkungan. Ini memungkinkan pemeliharaan

yang lebih mudah dan efisiensi jaringan yang lebih tinggi karena paket data dapat dirutekan berdasarkan hirarki yang telah ditentukan.

Hierarki ini juga meningkatkan keamanan jaringan karena perangkat dalam kelompok tertentu dapat diatur untuk berkomunikasi hanya dengan kelompoknya atau dengan perangkat tertentu, mengurangi risiko akses yang tidak diinginkan dari luar jaringan.

Pengelolaan alamat IP yang efisien memengaruhi secara langsung performa jaringan IoT. Dengan menggunakan metode alokasi yang tepat dan struktur hirarki, lalu lintas data dapat dikurangi, kecepatan respons dapat meningkat, dan ketahanan jaringan terhadap kegagalan jaringan meningkat. Selain itu, pengaturan alamat IP yang tepat membantu dalam memantau dan mengelola perangkat, terutama dalam sistem yang membutuhkan pelacakan waktu nyata, seperti di bidang kesehatan atau transportasi.

Namun, pengelolaan alamat IP juga menghadirkan tantangan, khususnya pada jaringan IoT yang terus berkembang. Dengan semakin banyaknya perangkat yang terhubung, administrator jaringan perlu secara berkala memperbarui metode pengelolaan dan mempertimbangkan mekanisme otomatisasi, seperti perangkat lunak manajemen alamat IP (IPAM) yang secara otomatis mengelola alokasi, deteksi konflik, dan perubahan alamat IP di jaringan yang besar dan kompleks.

5.5 Protokol Pendukung untuk IP dalam IoT

Dalam jaringan IoT, protokol pendukung untuk komunikasi IP sangat diperlukan untuk memastikan bahwa perangkat dapat berkomunikasi secara efisien, aman, dan dapat diandalkan. Berbagai protokol digunakan untuk mendukung pengiriman data di lapisan jaringan dan aplikasi, dan setiap protokol memiliki karakteristik serta kegunaan tertentu yang disesuaikan dengan kebutuhan jaringan IoT.

Protokol TCP/IP dan UDP dalam Komunikasi IoT:

1. TCP (*Transmission Control Protocol*): TCP adalah protokol yang andal untuk pengiriman data, di mana setiap paket data dijamin sampai ke tujuan dengan urutan yang benar. TCP melakukan pengaturan ulang, koreksi kesalahan, dan pengelolaan koneksi untuk memastikan bahwa data yang dikirim dan diterima tidak rusak atau hilang. Namun, kekuatan TCP yang menjamin keandalan sering kali menjadi kelemahan dalam jaringan IoT, terutama untuk perangkat dengan keterbatasan sumber daya. Koneksi yang terus-menerus memakan bandwidth dan daya lebih tinggi, sehingga dalam banyak aplikasi IoT yang memerlukan pengiriman data cepat dan ringan, TCP bukanlah protokol yang paling efisien.
2. UDP (*User Datagram Protocol*): Sebagai alternatif yang lebih ringan dari TCP, UDP tidak memerlukan koneksi yang tetap dan tidak menjamin urutan atau keberhasilan pengiriman data. Protokol ini sesuai untuk aplikasi yang membutuhkan pengiriman data real-time atau memiliki toleransi terhadap kehilangan data, seperti sensor yang mengirim data lingkungan secara berkelanjutan. UDP lebih hemat daya dan bandwidth karena tidak memerlukan overhead untuk pengelolaan koneksi, yang sangat cocok untuk perangkat IoT yang memiliki daya terbatas dan memerlukan komunikasi sederhana.

Untuk memenuhi kebutuhan IoT, beberapa protokol yang lebih ringan dari TCP dan UDP dikembangkan khusus untuk mendukung keterbatasan sumber daya pada perangkat IoT, antara lain *Constrained Application Protocol* (CoAP) dan *Message Queuing Telemetry Transport* (MQTT):

1. *Constrained Application Protocol* (CoAP):
 - Definisi: CoAP adalah protokol lapisan aplikasi yang dirancang untuk perangkat IoT yang terhubung melalui jaringan yang terbatas, seperti sensor dan aktuator. Protokol ini berfungsi seperti HTTP tetapi dengan overhead

yang jauh lebih rendah, sehingga cocok untuk lingkungan IoT.

- Fitur Utama: CoAP mendukung metode permintaan sederhana seperti GET, POST, PUT, dan DELETE, mirip dengan HTTP, namun lebih hemat sumber daya. CoAP juga mendukung pengiriman *multicast*, yang digunakan untuk komunikasi grup dalam IoT.
- Keuntungan CoAP dalam IoT: CoAP memungkinkan komunikasi yang efisien antara perangkat dengan keterbatasan daya dan kapasitas, serta mendukung enkripsi menggunakan DTLS (*Datagram Transport Layer Security*), sehingga menjaga keamanan data pada perangkat IoT yang mungkin rentan terhadap serangan.

2. *Message Queuing Telemetry Transport* (MQTT):

- Definisi: MQTT adalah protokol yang berorientasi pesan, dirancang khusus untuk komunikasi jarak jauh dengan keterbatasan *bandwidth*. MQTT memungkinkan perangkat IoT mengirimkan data melalui model *publish-subscribe*, di mana perangkat dapat bertindak sebagai penerbit (*publisher*) atau pelanggan (*subscriber*) dari saluran data (*topic*) tertentu.
- Fitur Utama: Protokol ini dirancang untuk penggunaan daya rendah, cocok untuk perangkat IoT seperti sensor yang mungkin hanya mengirimkan data pada interval waktu tertentu. MQTT menggunakan mekanisme "*keep alive*" untuk menjaga koneksi yang ringan dan mendukung berbagai tingkat *Quality of Service* (QoS) agar data dapat dikirim secara andal atau hemat daya.
- Keuntungan MQTT dalam IoT: Karena protokol ini hemat *bandwidth* dan ringan, MQTT sering digunakan dalam aplikasi seperti pelacakan lokasi atau pemantauan lingkungan. Fleksibilitasnya dalam mengelola data melalui model *publish-subscribe* membuatnya ideal untuk jaringan IoT yang besar dengan kebutuhan komunikasi satu-ke-banyak.

Penggunaan protokol dalam jaringan IoT sering kali disesuaikan dengan skenario dan kebutuhan aplikasi tertentu. Misalnya, sensor lingkungan yang hanya membutuhkan pengiriman data yang sederhana dan tidak terlalu kritis dapat menggunakan UDP atau CoAP, yang lebih hemat daya dan tidak memerlukan keandalan yang tinggi. Sementara itu, aplikasi yang lebih sensitif terhadap data seperti pemantauan kesehatan mungkin memerlukan MQTT dengan pengaturan QoS yang lebih tinggi untuk memastikan data yang dikirim sampai secara akurat dan konsisten.

Selain itu, dalam jaringan IoT skala besar, penggunaan kombinasi protokol juga umum diterapkan. Protokol yang lebih ringan seperti CoAP dan MQTT dapat digunakan di perangkat-perangkat ujung (*edge devices*), sementara protokol yang lebih andal seperti TCP bisa diterapkan pada lapisan gateway atau server untuk menjamin pengelolaan data yang lebih aman dan terstruktur.

5.6 Keamanan IP pada IoT

Seiring dengan peningkatan jumlah perangkat yang terhubung dalam jaringan IoT, keamanan IP menjadi salah satu perhatian utama. Banyak perangkat IoT yang terhubung melalui IP rentan terhadap serangan siber, seperti peretasan, penyusupan data, dan penyalahgunaan informasi. Dalam konteks jaringan IoT, menjaga keamanan pada level IP sangat diperlukan karena banyak perangkat IoT memiliki daya komputasi dan kapasitas penyimpanan yang terbatas, sehingga sulit menerapkan protokol keamanan yang kuat. Pada halaman ini, kita akan membahas risiko utama keamanan IP pada IoT, teknik mitigasi yang dapat diterapkan, dan tantangan unik yang dihadapi dalam penerapan IPv6.

Beberapa risiko keamanan utama yang dihadapi dalam jaringan IoT di lapisan IP meliputi:

1. Serangan DDoS (*Distributed Denial of Service*): Serangan DDoS adalah jenis serangan di mana perangkat IoT yang terhubung di bawah satu alamat IP ditargetkan dengan jumlah lalu lintas yang sangat tinggi hingga layanan jaringan terganggu atau mati. Dengan banyaknya perangkat yang terhubung dalam jaringan IoT, DDoS dapat menyebabkan kerugian besar, terutama jika perangkat tersebut terkait dengan infrastruktur kritis seperti energi atau kesehatan.
2. *Spoofing Alamat IP*: *Spoofing* adalah metode di mana peretas mencoba menyamar sebagai perangkat lain dalam jaringan dengan meniru alamat IP perangkat asli. Ini bisa menyebabkan komunikasi antar perangkat terancam, atau data sensitif berpotensi diakses oleh pihak yang tidak berwenang. Dalam jaringan IoT, *spoofing* IP dapat memungkinkan akses tidak sah ke perangkat dan data mereka, menimbulkan ancaman besar bagi privasi pengguna.
3. Penyadapan Data: Karena komunikasi antar perangkat IoT sering kali berjalan secara langsung melalui jaringan IP, data yang dikirimkan melalui jaringan dapat disadap. Ini bisa sangat berbahaya jika data yang dikirim mencakup informasi pribadi atau sensitif. Penyadapan ini menjadi lebih berisiko pada perangkat IoT yang mungkin tidak memiliki enkripsi data yang kuat.

Dalam rangka mengatasi risiko-risiko di atas, terdapat beberapa teknik mitigasi yang dapat diterapkan pada jaringan IoT:

1. Firewall dan Sistem Deteksi Intrusi (IDS): *Firewall* merupakan teknik perlindungan dasar yang dapat memblokir akses tidak sah ke jaringan. Dalam IoT, *firewall* dapat ditempatkan pada lapisan *gateway* atau *server* yang mengelola perangkat IoT untuk mencegah akses dari IP yang

mencurigakan. Selain itu, sistem deteksi intrusi (IDS) dapat digunakan untuk memantau jaringan secara terus-menerus dan mendeteksi anomali yang mungkin mengindikasikan adanya serangan.

2. Enkripsi Data dengan IPsec: IPsec adalah protokol keamanan yang memungkinkan enkripsi dan autentikasi data pada lapisan IP. Penggunaan IPsec dalam jaringan IoT dapat memastikan bahwa data yang dikirim antar perangkat aman dan tidak dapat diakses oleh pihak ketiga. Dengan enkripsi yang diaktifkan, bahkan jika data disadap, informasinya tetap tidak dapat dibaca tanpa kunci enkripsi yang benar. IPsec khususnya mendukung IPv6, sehingga lebih mudah diterapkan pada jaringan IoT berbasis IPv6.
3. Autentikasi Alamat IP: Autentikasi adalah langkah kritis dalam melindungi jaringan IoT dari spoofing IP. Dengan menggunakan teknik autentikasi, perangkat IoT perlu membuktikan identitas mereka sebelum mengirim atau menerima data, sehingga hanya perangkat yang sah yang dapat mengakses jaringan. Teknologi seperti *digital certificates* (sertifikat digital) dan kunci enkripsi publik dapat diterapkan untuk memastikan bahwa perangkat yang terhubung adalah perangkat yang sah.

5.7 Pemanfaatan IP Multicast dalam IoT

Dalam jaringan IoT, IP *multicast* merupakan metode yang digunakan untuk mengirim data secara efisien ke beberapa perangkat sekaligus tanpa perlu membuat salinan data yang terpisah untuk setiap perangkat. Pendekatan ini memungkinkan distribusi data dalam jumlah besar secara cepat ke berbagai perangkat, yang sangat relevan dalam aplikasi yang membutuhkan sinkronisasi informasi secara *real-time* atau penyebaran data ke beberapa node IoT yang tersebar di area tertentu.

IP *multicast* adalah metode komunikasi di mana data dikirim dari satu sumber ke beberapa perangkat penerima sekaligus, yang tergabung dalam grup *multicast* tertentu. Berbeda dengan komunikasi *unicast* (satu-ke-satu) atau *broadcast* (satu-ke-semua), *multicast* memungkinkan komunikasi satu-ke-banyak secara selektif, yang dapat menghemat *bandwidth* dan mengurangi beban jaringan. IP *multicast* bekerja dengan cara:

1. *Grup Multicast*: Sumber data mengirim data ke alamat IP *multicast* tertentu, yang hanya diterima oleh perangkat yang telah mendaftar pada grup *multicast* tersebut.
2. *Routing Multicast*: Router di dalam jaringan *multicast* merutekan data hanya ke perangkat yang terdaftar pada grup, menghindari pengiriman ke perangkat yang tidak membutuhkan data tersebut.
3. *Membership Management*: Protokol seperti IGMP (*Internet Group Management Protocol*) digunakan untuk mengelola keanggotaan grup *multicast*, memastikan perangkat dapat bergabung dan meninggalkan grup sesuai kebutuhan.

Penggunaan IP *multicast* di jaringan IoT memberikan beberapa keuntungan utama, antara lain:

1. Efisiensi *Bandwidth*: Dengan *multicast*, data hanya perlu dikirim sekali, meskipun ada banyak penerima. Hal ini mengurangi penggunaan *bandwidth* secara signifikan, terutama pada jaringan IoT skala besar yang memiliki banyak perangkat yang memerlukan data yang sama.
2. Reduksi Beban pada Sumber Data: *Multicast* mengurangi beban pada sumber data atau server, karena data tidak perlu diduplikasi untuk setiap penerima. Hal ini sangat bermanfaat dalam jaringan IoT di mana perangkat sumber mungkin memiliki daya dan sumber daya terbatas.
3. Pengurangan Latensi: Dalam aplikasi yang membutuhkan respons cepat, *multicast* dapat mengurangi latensi dengan menghindari pengiriman data berulang ke beberapa

perangkat, sehingga memungkinkan pengiriman data yang cepat ke semua perangkat dalam grup *multicast*.

5.8 IP dan Pengoptimalan Jaringan pada IoT

Optimalisasi jaringan adalah kunci dalam pengelolaan perangkat IoT yang beroperasi dalam jaringan IP, terutama karena banyak perangkat IoT memiliki keterbatasan dalam hal daya, bandwidth, dan kapasitas pemrosesan. Pada jaringan IoT yang melibatkan ribuan hingga jutaan perangkat, optimalisasi IP memungkinkan jaringan berfungsi secara efisien tanpa membebani perangkat atau menurunkan kualitas layanan.

Dalam jaringan IoT, efisiensi adalah aspek krusial yang dapat dicapai melalui beberapa strategi optimalisasi IP, antara lain:

1. **Pengelompokan atau *Clustering* Perangkat:** Dalam jaringan yang besar, perangkat IoT dapat dikelompokkan berdasarkan lokasi, fungsi, atau jenis layanan. Dengan pengelompokan ini, komunikasi antar perangkat dalam satu kelompok atau *cluster* dapat dioptimalkan melalui jalur terpendek. Selain itu, perangkat yang berfungsi sebagai pengumpul data di dalam cluster dapat mengirimkan data yang sudah diproses ke server pusat, mengurangi lalu lintas data yang tidak perlu.
2. **Penggunaan Protokol IP yang Ringan:** Untuk menghemat sumber daya, protokol komunikasi yang lebih ringan seperti UDP, CoAP, atau MQTT sering digunakan, tergantung pada kebutuhan aplikasi. Misalnya, UDP tidak memerlukan proses verifikasi koneksi seperti pada TCP, sehingga lebih hemat bandwidth dan daya. Protokol seperti CoAP dan MQTT mendukung pendekatan komunikasi yang lebih hemat energi, ideal untuk perangkat dengan keterbatasan daya.
3. **Penerapan Alamat IP Dinamis:** Menggunakan metode alokasi IP dinamis dengan protokol seperti DHCP memungkinkan

perangkat mendapatkan alamat IP hanya saat diperlukan. Dengan begitu, perangkat yang tidak aktif atau jarang beroperasi tidak perlu terhubung secara terus-menerus, yang dapat mengurangi beban pada jaringan.

Routing adalah komponen utama dalam jaringan IoT yang menentukan jalur komunikasi antar perangkat dan menuju server pusat. Teknik routing yang efisien tidak hanya membantu mempercepat pengiriman data, tetapi juga menghemat daya dan bandwidth jaringan. Beberapa teknik routing yang relevan dalam jaringan IoT adalah:

1. *Routing Berbasis Cluster (Cluster-Based Routing)*: Dalam pendekatan ini, jaringan IoT dibagi menjadi beberapa *cluster* atau kelompok perangkat. Setiap *cluster* memiliki pemimpin (*cluster head*) yang bertanggung jawab untuk mengumpulkan data dari anggota *cluster* dan meneruskannya ke server pusat. Pendekatan ini mengurangi jumlah perangkat yang harus berkomunikasi langsung dengan server, sehingga menghemat daya dan bandwidth.
2. *Routing Adaptif Berdasarkan Energi (Energy-Aware Routing)*: Teknik ini dirancang untuk jaringan IoT dengan perangkat yang memiliki keterbatasan daya. Dalam *energy-aware routing*, perangkat memilih jalur berdasarkan tingkat energi yang tersedia, memilih jalur yang paling hemat energi untuk menghindari perangkat yang hampir habis dayanya. Teknik ini membantu memperpanjang masa operasional perangkat IoT.
3. *Routing Berdasarkan Kualitas Layanan (QoS-Aware Routing)*: Teknik routing ini mempertimbangkan kebutuhan kualitas layanan (*Quality of Service*) dalam menentukan jalur komunikasi. Misalnya, perangkat yang membutuhkan pengiriman data real-time akan diprioritaskan untuk jalur dengan latensi rendah. Teknik ini relevan dalam IoT karena beberapa aplikasi, seperti pemantauan kesehatan atau

transportasi cerdas, membutuhkan komunikasi yang cepat dan andal.

Salah satu strategi optimalisasi yang semakin populer dalam jaringan IoT adalah *edge computing*, di mana sebagian pemrosesan data dilakukan di perangkat ujung (*edge devices*) daripada mengirim semua data ke server pusat. Dengan *edge computing*, perangkat IoT dapat memproses dan menyaring data sebelum dikirim, mengurangi jumlah data yang harus melalui jaringan IP. Pendekatan ini tidak hanya menghemat *bandwidth*, tetapi juga mengurangi latensi, yang berguna dalam aplikasi yang membutuhkan respons cepat.

Misalnya, dalam aplikasi *smart home*, perangkat sensor dapat menganalisis data lingkungan dan hanya mengirimkan peringatan jika kondisi tertentu tercapai, seperti suhu yang mencapai ambang batas. Dengan demikian, *edge computing* mengurangi frekuensi komunikasi yang tidak perlu, menghemat daya perangkat dan meningkatkan efisiensi jaringan.

5.9 Kesimpulan

Internet Protocol (IP) sebagai lapisan jaringan di IoT berfungsi sebagai pondasi yang memungkinkan perangkat dari berbagai jenis dan fungsi dapat terhubung, berbagi data, dan berkomunikasi secara aman dan efisien. Tanpa IP, pengelolaan jaringan IoT dalam skala besar tidak akan mungkin dilakukan dengan cara yang efektif. Seiring dengan pertumbuhan IoT di berbagai sektor, kebutuhan akan protokol yang fleksibel, aman, dan efisien menjadi kebutuhan utama, dan IP, terutama dengan evolusi IPv6, terbukti mampu memenuhi sebagian besar kebutuhan tersebut.

Keberhasilan implementasi IP di IoT memerlukan perhatian terhadap tantangan-tantangan yang telah dijelaskan, seperti keamanan, pengelolaan sumber daya, dan skalabilitas. Organisasi dan pengembang IoT perlu mengadopsi strategi yang efisien, seperti penggunaan protokol hemat daya, optimalisasi

algoritma *routing*, serta pendekatan keamanan yang disesuaikan dengan kemampuan perangkat IoT.

Dengan pendekatan yang tepat, IP akan terus menjadi lapisan jaringan utama yang menggerakkan IoT, menghubungkan berbagai perangkat di seluruh dunia, dari rumah pintar hingga industri besar. Di masa depan, dengan adanya inovasi dalam standar dan teknologi, jaringan IoT berbasis IP akan menjadi lebih aman, efisien, dan terintegrasi, mendukung kemajuan teknologi di berbagai aspek kehidupan.

DAFTAR PUSTAKA

- Abood, A.M., Hasan, W.K. and Khaled, H. (2024), "6LoWPAN - Technical Features and Challenges in IoT: A Review", *2024 IEEE 4th International Maghreb Meeting of the Conference on Sciences and Techniques of Automatic Control and Computer Engineering, MI-STA 2024 - Proceeding*, pp. 476–481, doi: 10.1109/MI-STA61267.2024.10599740.
- Giambene, G. (2021), "IP-Based Networks and Future Trends", *Textbooks in Telecommunications Engineering*, Vol. Part F1373, pp. 65–182, doi: 10.1007/978-3-030-75973-5_2.
- Kayyali, M. (2022), "Internet of Things (IoT): Emphasizing Its Applications and Emergence in Environmental Management-The Profound Cases", *Environmental Informatics: Challenges and Solutions*, pp. 201–212, doi: 10.1007/978-981-19-2083-7_11.
- Mali, A. and Nimkar, A. (2017), "Security Schemes for Constrained Application Protocol in IoT: A Precise Survey", *Communications in Computer and Information Science*, Vol. 746, pp. 134–145, doi: 10.1007/978-981-10-6898-0_11.
- Patel, A., Shanmugapriya, D., Srivastava, G. and Lin, J.C.W. (2021), "Routing Protocol Security for Low-Power and Lossy Networks in the Internet of Things", *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, Vol. 13147 LNCS, pp. 133–145, doi: 10.1007/978-3-030-93620-4_11.
- Sivaraman, V., Gharakheili, H.H., Fernandes, C., Clark, N. and Karlychuk, T. (2018), "Smart IoT Devices in the Home: Security and Privacy Implications", *IEEE Technology and Society Magazine*, Vol. 37 No. 2, pp. 71–79, doi: 10.1109/MTS.2018.2826079.

- Tian, Y.C. and Gao, J. (2024), "Network Addressing Architecture", *Signals and Communication Technology*, Vol. Part F1492, pp. 161–219, doi: 10.1007/978-981-99-5648-7_6.
- Verma, A., Verma, P., Farhaoui, Y. and Lv, Z. (2022), *Emerging Real-World Applications of Internet of Things*, *Emerging Real-World Applications of Internet of Things*, doi: 10.1201/9781003304203.

BAB 6

PROTOKOL APLIKASI PADA IoT

Oleh Tasrif Hasanuddin

6.1 Pendahuluan

Internet of Things (IoT) terus berkembang dengan semakin banyaknya perangkat yang saling terhubung dan berinteraksi untuk bertukar data dalam jumlah besar. Agar komunikasi antarperangkat ini berlangsung secara efektif dan efisien, diperlukan protokol aplikasi yang berfungsi sebagai penghubung antara perangkat IoT dan jaringan. Berbeda dengan protokol komunikasi jaringan tradisional, protokol yang digunakan dalam IoT harus dirancang agar sesuai dengan keterbatasan sumber daya yang dimiliki oleh perangkat, seperti daya baterai, kapasitas pemrosesan, dan bandwidth jaringan (Tennina *et al.*, 2013).

Dalam sistem IoT, protokol aplikasi memainkan peran penting dalam mengatur bagaimana data dikirim dan diterima antara perangkat serta layanan cloud. Keberagaman perangkat IoT dengan spesifikasi yang berbeda memerlukan protokol komunikasi yang ringan, fleksibel, dan memiliki tingkat keamanan tinggi. Tantangan utama dalam memilih protokol aplikasi meliputi efisiensi penggunaan energi, ketahanan terhadap latensi jaringan, keamanan dalam pertukaran data, serta kemampuan untuk menangani jutaan hingga miliaran perangkat yang saling terhubung dalam satu ekosistem (Sultan *et al.*, 2022).

Sebagian besar protokol aplikasi IoT bekerja di atas protokol jaringan seperti TCP/IP atau UDP, namun telah dioptimalkan agar lebih sesuai dengan karakteristik IoT. Beberapa protokol utama yang umum digunakan dalam ekosistem IoT antara lain MQTT (*Message Queuing Telemetry Transport*), CoAP (*Constrained Application Protocol*), HTTP/HTTPS (*HyperText Transfer Protocol*) (Peters, Jandrić and Hayes, 2022). Masing-masing protokol ini memiliki karakteristik unik yang membuatnya lebih sesuai untuk kasus penggunaan tertentu.

Sebagai contoh, MQTT merupakan salah satu protokol yang paling banyak digunakan dalam IoT karena sifatnya yang ringan dan efisien untuk komunikasi berbasis *publish-subscribe* (Tavasszy and Piecyk, 2018). Protokol ini sangat cocok untuk sistem yang memerlukan pengiriman data secara *real-time* dengan konsumsi *bandwidth* rendah, seperti pemantauan lingkungan, *smart home*, dan otomasi industri. Sementara itu, CoAP merupakan protokol berbasis REST yang lebih efisien dibandingkan HTTP, sehingga ideal untuk perangkat dengan keterbatasan daya dan kapasitas pemrosesan seperti sensor nirkabel (Tsai, 2019).

Meskipun memiliki *overhead* yang lebih besar, HTTP/HTTPS tetap banyak digunakan dalam sistem IoT yang berbasis web dan layanan *cloud*. AMQP, yang umumnya diterapkan dalam aplikasi *enterprise* dan perbankan, juga dapat digunakan dalam IoT untuk komunikasi yang menuntut keandalan tinggi (Blanchette and Merz, 2016). Sementara itu, DDS lebih sesuai untuk sistem yang memerlukan komunikasi *real-time* dengan latensi sangat rendah, seperti kendaraan otonom dan industri manufaktur yang mengandalkan otomatisasi tinggi (Kordon and Lemoine, 2004).

Pemilihan protokol aplikasi yang sesuai sangat bergantung pada kebutuhan spesifik dari implementasi IoT yang dikembangkan. Misalnya, sistem pemantauan lingkungan yang bergantung pada sensor berdaya rendah akan lebih optimal jika

menggunakan CoAP atau MQTT dibandingkan HTTP karena efisiensi daya dan *bandwidth*nya. Sebaliknya, sistem yang berinteraksi langsung dengan pengguna, seperti dashboard pemantauan berbasis web, lebih cocok menggunakan HTTP atau *WebSocket* untuk memastikan aksesibilitas yang lebih luas.

Bab ini akan mengulas berbagai protokol aplikasi yang umum digunakan dalam IoT, termasuk arsitektur, cara kerja, keunggulan, serta keterbatasan masing-masing protokol. Selain itu, pembahasan juga akan mencakup skenario penerapan yang paling sesuai untuk setiap protokol guna membantu pengembang dan praktisi IoT dalam menentukan pilihan yang paling tepat. Dengan pemahaman mendalam mengenai protokol aplikasi IoT, diharapkan pembaca dapat merancang sistem yang lebih efisien, andal, dan aman untuk mendukung ekosistem perangkat terhubung di era digital ini.

6.2 Protokol MQTT (*Message Queuing Telemetry Transport*)

Salah satu keunggulan utama MQTT adalah model komunikasi *publish-subscribe*, yang lebih efisien dibandingkan model *client-server* tradisional. Model ini melibatkan tiga komponen utama:

1. *Publisher* (Pengirim Data) – Perangkat yang mengirimkan data ke suatu topik.
2. *Broker* – *Server* yang bertindak sebagai perantara yang mendistribusikan pesan dari publisher ke subscriber.
3. *Subscriber* (Penerima Data) – Perangkat yang berlangganan ke suatu topik dan menerima pesan yang dikirimkan oleh broker.

Ketika *publisher* mengirimkan data ke suatu topik, *broker* akan meneruskan pesan tersebut ke semua subscriber yang berlangganan pada topik yang sama. Model ini membuat komunikasi lebih fleksibel dan efisien karena perangkat tidak perlu mengetahui alamat satu sama lain.

Broker berperan penting dalam sistem MQTT dengan fungsi utama sebagai berikut:

- Menerima pesan dari *publisher*.
- Menyimpan sementara pesan (jika QoS mendukung).
- Mendistribusikan pesan ke subscriber yang relevan.

Dalam sistem MQTT, *broker* adalah komponen utama yang bertanggung jawab untuk menerima, menyimpan, dan meneruskan pesan antara *publisher* dan *subscriber*.

6.2.1 Mosquitto

Mosquitto adalah broker MQTT open-source yang ringan dan cocok untuk perangkat dengan sumber daya terbatas. Dikembangkan oleh Eclipse Foundation, Mosquitto mendukung protokol MQTT v3.1, v3.1.1, dan v5.0. Kelebihannya adalah:

- Ringan dan cepat, cocok untuk *embedded system* dan perangkat IoT kecil.
- Mudah diinstal di berbagai platform seperti Linux, Windows, dan macOS.
- Dukungan TLS/SSL untuk keamanan komunikasi.

Namun, Mosquitto kurang optimal untuk skala besar karena tidak mendukung clustering secara bawaan.

6.2.2. EMQX

EMQX (*Erlang MQTT Broker*) adalah broker MQTT *open-source* berbasis Erlang yang sangat *scalable*. Keunggulannya:

- Mendukung *clustering* hingga jutaan perangkat IoT.
- Dukungan multi-protokol, termasuk MQTT, HTTP, dan WebSocket.
- Fitur monitoring dan analitik yang kuat.

EMQX cocok untuk aplikasi skala besar seperti IoT industri dan *smart city*.

6.2.3 HiveMQ

HiveMQ adalah broker MQTT *enterprise-grade* yang dirancang untuk keandalan tinggi dan integrasi *cloud*. Fitur utama:

- Dukungan clustering yang stabil untuk beban tinggi.
- Integrasi dengan Kafka dan *cloud services* seperti AWS dan Azure.
- Manajemen akses berbasis kontrol peran (RBAC).

HiveMQ cocok untuk perusahaan yang membutuhkan solusi *robust* dan berkeamanan tinggi.

6.2.4 AWS IoT Core

AWS IoT Core adalah broker MQTT berbasis cloud yang dikelola oleh Amazon Web Services (AWS). Fitur utamanya:

- *Serverless*, tidak memerlukan pengelolaan infrastruktur.
- Terintegrasi dengan layanan AWS, seperti Lambda, S3, dan DynamoDB.
- Keamanan bawaan dengan sertifikat dan autentikasi perangkat. AWS IoT Core ideal untuk aplikasi IoT berbasis *cloud* dengan skala global.

6.2.5 Quality of Service (QoS) dalam MQTT

Quality of Service (QoS) dalam MQTT (*Message Queuing Telemetry Transport*) adalah mekanisme yang menentukan tingkat keandalan dalam pengiriman pesan antara publisher dan subscriber melalui broker. QoS ini penting dalam sistem IoT, karena memastikan bahwa pesan dapat dikirim dengan tingkat kepastian tertentu, tergantung pada kebutuhan aplikasi. MQTT mendukung tiga tingkat QoS, yaitu QoS 0 (*At Most Once*), QoS 1 (*At Least Once*), dan QoS 2 (*Exactly Once*).

➤ **QoS 0 – At Most Once (Paling Banyak Sekali)**

QoS 0 adalah tingkat paling rendah dalam QoS MQTT, di mana pesan dikirimkan tanpa jaminan penerimaan oleh penerima. *Publisher* mengirimkan pesan ke broker, dan broker meneruskannya ke *subscriber* tanpa mekanisme pengakuan atau pengiriman ulang jika pesan gagal dikirim.

Mekanisme Kerja

1. *Publisher* mengirim pesan ke broker tanpa menunggu konfirmasi.
2. Broker meneruskan pesan ke *subscriber* tanpa ada pengakuan dari *subscriber*.
3. Jika pesan hilang selama transmisi, pesan tidak akan dikirim ulang.

Kelebihan

1. Sangat cepat dan efisien karena tidak ada overhead komunikasi tambahan.
2. Cocok untuk jaringan dengan bandwidth terbatas karena mengurangi lalu lintas jaringan.
3. Ideal untuk data yang tidak kritis, seperti pembacaan sensor berkala atau data yang diperbarui terus-menerus (misalnya, suhu ruangan yang diperbarui setiap detik).

Kekurangan

1. Tidak ada jaminan bahwa pesan akan diterima oleh *subscriber*.
2. Jika jaringan terputus, pesan akan hilang.

Contoh Penggunaan

1. Pemantauan lingkungan dengan sensor suhu yang mengirim data berkala.
2. Streaming data yang tidak memerlukan keandalan tinggi (seperti data cuaca).

➤ **QoS 1 – At Least Once (Minimal Sekali)**

QoS 1 memastikan bahwa pesan akan dikirim minimal satu kali, tetapi dapat dikirim lebih dari satu kali jika konfirmasi penerimaan tidak diterima oleh publisher atau broker. Ini berarti bahwa penerima mungkin menerima duplikasi pesan, tetapi tidak akan kehilangan pesan sepenuhnya.

Mekanisme Kerja

1. *Publisher* mengirimkan pesan ke broker dan menunggu konfirmasi penerimaan (PUBACK).
2. Jika tidak ada konfirmasi dalam waktu tertentu, *publisher* akan mengirim ulang pesan.
3. Broker mengirimkan pesan ke subscriber dan menunggu konfirmasi.
4. Jika subscriber tidak mengirim konfirmasi, broker akan mengirim ulang pesan.

Kelebihan

1. Menjamin bahwa pesan tidak akan hilang, meskipun dapat terjadi duplikasi.
2. Cocok untuk aplikasi yang memerlukan tingkat keandalan sedang.
3. Menggunakan sedikit lebih banyak *bandwidth* dibandingkan QoS 0, tetapi tetap efisien.

Kekurangan

1. Pesan dapat dikirim lebih dari sekali (duplikasi), yang bisa mempengaruhi aplikasi tertentu.
2. Menggunakan lebih banyak *bandwidth* dan daya dibandingkan QoS 0.

Contoh Penggunaan

- Sistem notifikasi IoT, misalnya alarm kebakaran yang harus dikirim meskipun berisiko terjadi duplikasi.
- Pemantauan kendaraan dalam *fleet management*, di mana informasi lokasi harus dikirim meskipun terjadi jaringan yang tidak stabil.

➤ **QoS 2 – *Exactly Once* (Tepat Sekali)**

QoS 2 adalah tingkat keandalan tertinggi dalam MQTT, di mana pesan dijamin akan dikirim dan diterima hanya satu kali. Untuk mencapai ini, MQTT menggunakan mekanisme handshake yang lebih kompleks untuk memastikan tidak ada duplikasi maupun kehilangan pesan.

Mekanisme Kerja

1. Publisher mengirim pesan ke broker dengan permintaan konfirmasi penerimaan awal (PUBREC).
2. Broker merespons dengan PUBREC untuk mengonfirmasi bahwa pesan telah diterima.
3. Publisher mengirimkan PUBREL (*release message*) untuk memberi tahu broker bahwa pesan dapat diteruskan.
4. Broker mengirimkan PUBCOMP (*complete message*) kepada *publisher* untuk menutup transaksi.

Kelebihan

1. Menjamin bahwa pesan akan dikirim dan diterima tepat satu kali.
2. Tidak ada risiko kehilangan atau duplikasi pesan.
3. Sangat cocok untuk aplikasi yang memerlukan integritas data tinggi.

Kekurangan

1. Lebih lambat dibandingkan QoS 0 dan QoS 1, karena menggunakan lebih banyak langkah dalam pengiriman pesan.
2. Membutuhkan lebih banyak bandwidth dan daya pemrosesan.

Contoh Penggunaan

- Transaksi keuangan dalam IoT, seperti pembayaran melalui perangkat IoT yang harus diproses tepat satu kali.

- Sistem kontrol industri, di mana pengiriman instruksi ke mesin harus dilakukan dengan sangat akurat tanpa risiko duplikasi.

Tabel 6. 1 Perbandingan QoS Level pada MQTT

QoS Level	Jaminan Pengiriman	Kemungkinan Duplikasi	Kecepatan	Overhead	Contoh Penggunaan	QoS Level
QoS 0	Tidak ada jaminan	Tidak ada	Sangat cepat	Rendah	Data sensor berkala, notifikasi ringan	QoS 0
QoS 1	Minimal sekali	Mungkin ada	Cepat	Sedang	Alarm kebakaran, pemantauan kendaraan	QoS 1
QoS 2	Tepat satu kali	Tidak ada	Lambat	Tinggi	Transaksi IoT, kontrol industri	QoS 2

Pemilihan QoS dalam MQTT sangat bergantung pada kebutuhan spesifik aplikasi IoT.

Gunakan QoS 0 jika kecepatan lebih penting daripada keandalan, seperti pada pemantauan sensor yang mengirim data berkala.

- Gunakan QoS 1 jika pesan harus dikirim minimal sekali, meskipun ada risiko duplikasi, seperti pada sistem peringatan dini.
- Gunakan QoS 2 jika keakuratan pesan sangat penting dan duplikasi tidak boleh terjadi, seperti dalam transaksi keuangan atau kontrol mesin otomatis.

6.2.6 Keunggulan dan Kelemahan MQTT

MQTT (*Message Queuing Telemetry Transport*) adalah protokol komunikasi yang dirancang untuk perangkat dengan keterbatasan sumber daya dan jaringan dengan latensi tinggi atau bandwidth rendah. MQTT memiliki banyak keunggulan yang membuatnya populer dalam aplikasi *Internet of Things* (IoT), tetapi juga memiliki

beberapa kelemahan yang perlu diperhatikan dalam implementasinya.

Ringan dan Hemat *Bandwidth*

MQTT menggunakan overhead data yang sangat kecil dibandingkan protokol lain seperti HTTP. Ukuran paket data dalam MQTT jauh lebih kecil, karena:

1. Tidak memiliki header yang besar seperti dalam HTTP.
2. Menggunakan binary format untuk komunikasi, bukan teks seperti HTTP.
3. Tidak memerlukan mekanisme request-response yang kompleks.

Contoh: Dalam aplikasi IoT seperti smart home, sensor suhu dapat mengirimkan data menggunakan MQTT hanya dengan beberapa byte, sementara HTTP akan menggunakan beberapa kilobyte untuk paket yang sama.

Efisien dalam Penggunaan Daya

MQTT sangat cocok untuk perangkat dengan daya terbatas, seperti sensor IoT yang menggunakan baterai atau perangkat *low-power* seperti ESP8266 dan ESP32. Mengapa hemat daya? MQTT memungkinkan komunikasi asinkron melalui model *publish-subscribe*, sehingga perangkat tidak perlu mempertahankan koneksi terus-menerus seperti HTTP. MQTT mendukung fitur *Keep Alive* yang memungkinkan perangkat tidur (*sleep mode*) saat tidak aktif, sehingga menghemat daya baterai. Contoh: Perangkat IoT yang menggunakan baterai dapat menghemat energi dengan hanya mengirim data secara berkala dan masuk ke mode deep sleep ketika tidak diperlukan.

Model *Publish-Subscribe* yang Fleksibel

MQTT menggunakan arsitektur *publish-subscribe*, yang berbeda dengan model request-response seperti dalam HTTP.

Keunggulan model ini:

1. *Subscriber* tidak perlu mengetahui alamat publisher, sehingga lebih fleksibel.
2. Satu publisher dapat mengirim pesan ke banyak *subscriber* tanpa harus membuat koneksi individual ke masing-masing perangkat.
3. *Subscriber* hanya menerima pesan dari topik yang relevan, mengurangi beban komunikasi.

Contoh: Dalam sistem pemantauan cuaca, satu sensor dapat mengirimkan data ke banyak perangkat sekaligus, termasuk aplikasi seluler dan server pemrosesan data.

Mendukung Koneksi yang Tidak Stabil

MQTT dirancang untuk bekerja pada jaringan yang memiliki latensi tinggi atau koneksi yang sering terputus, seperti jaringan seluler, satelit, atau IoT berbasis LPWAN (LoRa, NB-IoT). Fitur yang membantu dalam jaringan tidak stabil:

1. QoS (*Quality of Service*) untuk menjamin pengiriman pesan.
2. *Retained Message* yang memungkinkan *subscriber* baru mendapatkan pesan terakhir yang disimpan oleh *broker*.
3. *Last Will and Testament* (LWT) yang memungkinkan broker mengirimkan pesan jika suatu perangkat tiba-tiba terputus dari jaringan.

Contoh: MQTT dapat tetap bekerja di lingkungan industri dengan gangguan jaringan, seperti pada sistem pemantauan mesin di lokasi tambang atau ladang minyak.

Mendukung Berbagai Perangkat dan Platform

MQTT kompatibel dengan berbagai perangkat embedded (ESP8266, Raspberry Pi, Arduino) serta mendukung cloud computing, termasuk AWS IoT Core, Google Cloud IoT, dan Microsoft Azure IoT Hub. Keunggulan

ini membuatnya mudah diintegrasikan dengan berbagai teknologi IoT.

Contoh: Perusahaan yang menggunakan berbagai perangkat dari vendor berbeda tetap dapat mengintegrasikan semuanya dengan menggunakan MQTT.

Skalabilitas Tinggi

MQTT dapat menangani jutaan perangkat terhubung dengan menggunakan clustering pada broker MQTT seperti EMQX, HiveMQ, dan VerneMQ.

Contoh: MQTT digunakan dalam Smart City untuk menghubungkan sensor lalu lintas, CCTV, dan sistem transportasi publik dalam satu platform.

Tidak Memiliki *Native Security* (Keamanan Bawaan)

MQTT tidak memiliki enkripsi bawaan, sehingga harus dikombinasikan dengan TLS/SSL untuk keamanan data.

1. Risiko: Tanpa enkripsi, MQTT rentan terhadap *man-in-the-middle attack* dan *data interception* di jaringan terbuka.
2. Solusi: Implementasikan TLS/SSL dan gunakan autentikasi dengan *username/password* atau sertifikat digital.

Ketergantungan pada Broker

MQTT sangat bergantung pada broker sebagai perantara komunikasi. Jika broker mengalami kegagalan, seluruh komunikasi IoT dapat terputus.

Solusi:

1. Gunakan *clustering broker* MQTT untuk meningkatkan ketahanan sistem.
2. Pilih broker dengan fitur *high availability*, seperti HiveMQ atau AWS IoT Core.

Tidak Cocok untuk Transfer Data Besar

MQTT dirancang untuk **pesan kecil**, sehingga tidak optimal untuk mengirimkan file besar seperti video, gambar resolusi tinggi, atau log dalam jumlah besar. Solusi: Jika perlu mengirim data besar, gunakan kombinasi MQTT dengan HTTP atau FTP untuk mengunggah file.

Konfigurasi yang Bisa Rumit

Meskipun MQTT sederhana untuk perangkat kecil, pengaturan broker MQTT dalam sistem besar bisa rumit, terutama jika membutuhkan *clustering*, *load balancing*, dan *monitoring*. Solusi: Gunakan layanan cloud MQTT seperti AWS IoT Core atau EMQX Cloud untuk mengurangi kompleksitas pengelolaan.

Konsumsi Memori Lebih Tinggi dibandingkan UDP

Jika dibandingkan dengan UDP (*User Datagram Protocol*), MQTT memerlukan lebih banyak memori dan CPU, terutama saat menggunakan QoS 2 yang memiliki banyak tahapan *handshake*. Solusi: Gunakan QoS 0 atau QoS 1 jika perangkat memiliki keterbatasan memori.

6.2.7 Implementasi MQTT dalam IoT

Smart Home

Dalam *smart home*, MQTT menghubungkan perangkat pintar seperti lampu, termostat, dan kamera keamanan. Sebagai contoh, sensor suhu dapat mengirimkan data ke broker, lalu diteruskan ke aplikasi pengguna untuk ditampilkan secara *real-time*.

Industrial IoT (IIoT)

Di sektor industri, MQTT menghubungkan mesin, sensor, dan sistem pemantauan. Sistem ini memungkinkan pemantauan kondisi mesin secara otomatis serta memberikan peringatan dini jika terjadi kerusakan.

Transportasi dan *Fleet Management*

Dalam sistem transportasi, MQTT digunakan untuk memantau lokasi kendaraan, kondisi mesin, serta memberikan notifikasi dalam sistem manajemen armada. Dengan MQTT, kendaraan dapat mengirimkan data berkala tanpa harus mempertahankan koneksi terus-menerus.

Healthcare* dan *Medis

Dalam dunia medis, perangkat IoT berbasis MQTT membantu pemantauan pasien jarak jauh. Contohnya, perangkat wearable yang mengukur detak jantung dapat mengirimkan data ke sistem kesehatan melalui broker MQTT.

6.2.8 Keamanan MQTT

Enkripsi dengan TLS/SSL

Karena MQTT tidak memiliki enkripsi bawaan, implementasi keamanan dapat menggunakan *Transport Layer Security* (TLS) atau *Secure Sockets Layer* (SSL) untuk mengenkripsi komunikasi antarperangkat.

Autentikasi Pengguna

Broker MQTT dapat menggunakan mekanisme autentikasi berbasis *username* dan *password* atau sertifikat digital untuk memastikan hanya perangkat yang sah yang dapat berkomunikasi dalam jaringan.

***Firewall* dan Pembatasan Akses**

Untuk meningkatkan keamanan, sistem MQTT dapat menerapkan *firewall* atau membatasi alamat IP yang diperbolehkan untuk mengakses broker MQTT.

6.2.9 Kesimpulan

MQTT adalah protokol komunikasi yang efisien dan ringan untuk sistem IoT, dengan keunggulan utama pada penggunaan *bandwidth* rendah, fleksibilitas komunikasi, serta efisiensi daya. Dengan model *publish-subscribe*, MQTT memungkinkan komunikasi antarperangkat secara asinkron dan dapat beroperasi dengan baik pada jaringan yang tidak stabil.

Meskipun memiliki banyak manfaat, MQTT tetap memiliki beberapa keterbatasan, terutama dalam aspek keamanan dan ketergantungan pada broker. Oleh karena itu, penggunaan protokol keamanan tambahan seperti TLS/SSL, autentikasi pengguna, dan *firewall* sangat direkomendasikan untuk meningkatkan keamanan sistem.

Di masa depan, dengan semakin berkembangnya Internet of Things, MQTT diprediksi akan tetap menjadi salah satu protokol komunikasi utama dalam mendukung ekosistem perangkat terhubung yang lebih luas dan kompleks.

6.3 Constrained Application Protocol (CoAP)

Constrained Application Protocol (CoAP) adalah protokol komunikasi yang dirancang khusus untuk perangkat dengan sumber daya terbatas (*constrained devices*), seperti sensor dan aktuator dalam sistem *Internet of Things* (IoT). CoAP dikembangkan oleh *Internet Engineering Task Force* (IETF) dan diatur dalam standar RFC 7252. Protokol ini berfungsi pada model komunikasi *request-response*, mirip dengan HTTP, tetapi lebih ringan dan dioptimalkan untuk perangkat IoT dengan kapasitas komputasi, daya, dan *bandwidth* yang rendah.

CoAP dirancang untuk mendukung komunikasi machine-to-machine (M2M) dengan efisiensi tinggi, sekaligus memungkinkan perangkat yang terhubung untuk saling bertukar data menggunakan protokol berbasis internet.

Protokol ini sangat cocok untuk jaringan dengan bandwidth rendah, jaringan berbasis sensor, atau perangkat yang berjalan pada baterai kecil.

6.3.1 Arsitektur CoAP

CoAP dirancang untuk mengikuti model kerja HTTP dengan beberapa penyesuaian agar lebih ringan. Protokol ini menggunakan UDP (*User Datagram Protocol*) sebagai transport layer untuk mengurangi *overhead* komunikasi dan mendukung model komunikasi berikut:

1. *Request-Response*: Sama seperti HTTP, CoAP menggunakan metode seperti GET, POST, PUT, dan DELETE untuk berinteraksi dengan sumber daya.
2. *Asynchronous Messaging*: CoAP mendukung pesan asinkron untuk memastikan komunikasi tetap efisien meskipun ada latensi dalam jaringan.
3. *RESTful Interface*: CoAP dirancang berdasarkan prinsip *Representational State Transfer* (REST), memungkinkan sumber daya diakses melalui URI (*Uniform Resource Identifier*).

6.3.2 Fitur Utama CoAP

Protokol Berbasis UDP

Tidak seperti HTTP yang menggunakan TCP, CoAP menggunakan UDP untuk mengurangi *overhead* jaringan dan mempercepat transmisi data. UDP juga memungkinkan penggunaan daya yang lebih rendah, membuat CoAP cocok untuk perangkat IoT kecil.

Message Layer

CoAP menggunakan message layer untuk menangani reliabilitas dan urutan pengiriman pesan. Pesan dalam CoAP memiliki tipe berikut:

- *Confirmable* (CON): Pesan ini membutuhkan konfirmasi dari penerima. Jika tidak ada tanggapan, pesan akan dikirim ulang hingga penerima mengakui penerimaannya.
- *Non-confirmable* (NON): Pesan ini tidak memerlukan konfirmasi penerimaan dan cocok untuk data yang tidak kritis.
- *Acknowledgment* (ACK): Pesan balasan untuk mengonfirmasi penerimaan pesan CON.
- *Reset* (RST): Digunakan jika penerima tidak mengenali pesan atau tidak dapat memprosesnya.

Lightweight Header

Header CoAP hanya berukuran 4 byte, jauh lebih kecil dibandingkan HTTP, sehingga lebih hemat bandwidth dan daya.

Block-wise Transfer

CoAP memungkinkan pengiriman data dalam blok-blok kecil untuk mengakomodasi perangkat yang memiliki memori terbatas.

Caching

CoAP mendukung caching untuk mengurangi jumlah permintaan yang dikirimkan ke perangkat IoT, sehingga meningkatkan efisiensi komunikasi.

Multicast Support

CoAP mendukung multicast, memungkinkan satu pesan dikirim ke banyak perangkat sekaligus, sangat berguna dalam sistem IoT yang melibatkan banyak perangkat.

DTLS untuk Keamanan

CoAP menggunakan *Datagram Transport Layer Security* (DTLS) untuk memastikan keamanan data yang dikirimkan melalui jaringan.

6.3.3 Cara Kerja CoAP

Komunikasi dalam CoAP terjadi dalam dua langkah utama:

1. Request-Response

- Perangkat klien mengirimkan permintaan (*request*) ke server menggunakan metode seperti GET atau POST.
- Server kemudian mengirimkan respons berupa status kode (misalnya, "2.05 *Content*" untuk respons berhasil) dan data sumber daya yang diminta.

2. Pengelolaan Pesan

- Pesan-pesan yang membutuhkan konfirmasi dikirim sebagai *Confirmable* (CON). Jika respons tidak diterima dalam waktu tertentu, pesan dikirim ulang.
- Jika pesan tidak memerlukan konfirmasi, pesan dikirim sebagai *Non-confirmable* (NON) untuk efisiensi maksimum.

6.3.4 Keunggulan CoAP

Ringan dan Hemat *Bandwidth*

CoAP dirancang untuk perangkat dengan sumber daya terbatas, menggunakan header kecil (4 byte) dan UDP untuk mengurangi konsumsi *bandwidth*.

Efisien dalam Jaringan IoT

CoAP mendukung multicast dan asynchronous messaging, membuatnya sangat cocok untuk jaringan IoT skala besar dengan banyak perangkat.

RESTful dan Mudah Digunakan

CoAP berbasis REST memungkinkan pengembang memanfaatkan pendekatan yang sama seperti dalam HTTP, sehingga mudah diintegrasikan dengan sistem yang sudah ada.

***Caching* untuk Efisiensi**

Dukungan *caching* dalam CoAP mengurangi permintaan yang berulang ke perangkat IoT, sehingga menghemat daya dan *bandwidth*.

Dukungan Multicast

Multicast mempermudah komunikasi antara banyak perangkat IoT secara bersamaan, seperti dalam sistem smart home atau *smart city*.

Keamanan melalui DTLS

CoAP menggunakan DTLS untuk mengenkripsi pesan dan memastikan keamanan komunikasi dalam jaringan IoT yang rentan.

6.3.5 Kelemahan CoAP

Bergantung pada UDP

Meskipun UDP memiliki *overhead* yang rendah, ia tidak menyediakan jaminan pengiriman seperti TCP. Hal ini berarti CoAP harus mengelola reliabilitas pesan secara manual, yang dapat meningkatkan kompleksitas sistem.

Kompatibilitas Terbatas dengan Jaringan HTTP

CoAP tidak langsung kompatibel dengan HTTP, sehingga memerlukan proxy untuk menerjemahkan pesan antara CoAP dan HTTP jika diperlukan integrasi dengan sistem berbasis web.

Keamanan Bergantung pada DTLS

Meskipun CoAP mendukung DTLS untuk keamanan, konfigurasi DTLS dapat rumit dan meningkatkan *overhead* komunikasi.

Kurang Optimal untuk Data Besar

CoAP lebih cocok untuk data kecil, seperti pembacaan sensor. Untuk transfer data besar, seperti file atau gambar, protokol ini tidak optimal meskipun mendukung transfer berbasis blok.

6.3.6 Implementasi dan Penerapan CoAP

CoAP digunakan dalam berbagai aplikasi IoT yang melibatkan perangkat dengan sumber daya terbatas. Berikut beberapa contoh penerapan:

1. **Pemantauan Lingkungan**

CoAP sering digunakan dalam sistem pemantauan lingkungan, seperti sensor kualitas udara atau suhu, di mana data dikirimkan secara berkala dari perangkat ke server pusat. Contoh: Sensor kualitas udara mengirimkan data konsentrasi polutan ke server melalui permintaan GET pada URI tertentu.

2. **Smart Home**

Dalam sistem *smart home*, CoAP digunakan untuk mengontrol perangkat seperti lampu, termostat, dan sistem keamanan. Contoh: Aplikasi mobile mengirimkan permintaan POST ke lampu pintar untuk mengubah tingkat kecerahan.

3. **Jaringan Sensor Nirkabel**

CoAP sangat cocok untuk jaringan sensor nirkabel (*Wireless Sensor Networks*) yang memerlukan komunikasi efisien antar perangkat. Contoh: Sensor di ladang pertanian mengirimkan data kelembapan tanah menggunakan CoAP untuk menghemat *bandwidth*.

4. *Smart City*

Dalam sistem *smart city*, CoAP digunakan untuk mengelola perangkat IoT seperti lampu jalan pintar atau sistem parkir otomatis. Contoh: Sensor parkir mengirimkan data ketersediaan ruang parkir ke pusat kontrol melalui CoAP.

6.3.7 Kesimpulan

CoAP adalah protokol yang ideal untuk aplikasi IoT yang melibatkan perangkat dengan keterbatasan sumber daya. Dengan arsitektur ringan, dukungan *multicast*, dan kompatibilitas REST, CoAP menawarkan komunikasi yang efisien dalam sistem IoT skala besar. Namun, kelemahan seperti ketergantungan pada UDP dan kesulitan menangani data besar membuatnya kurang cocok untuk aplikasi yang memerlukan reliabilitas tinggi atau transfer data besar.

Untuk aplikasi IoT seperti *smart home*, pemantauan lingkungan, atau *smart city*, CoAP memberikan efisiensi tinggi dalam komunikasi antarperangkat. Namun, untuk aplikasi yang membutuhkan keandalan dan keamanan tingkat tinggi, kombinasi CoAP dengan protokol seperti DTLS atau integrasi dengan HTTP melalui proxy menjadi penting. Dengan pemahaman mendalam mengenai keunggulan dan kelemahan CoAP, pengembang dapat memanfaatkan protokol ini untuk merancang sistem IoT yang lebih hemat daya, ringan, dan *scalable*.

6.4 Protokol HTTP/HTTPS (*HyperText Transfer Protocol*)

HyperText Transfer Protocol (HTTP) adalah protokol komunikasi berbasis teks yang digunakan untuk mentransfer data melalui internet. HTTP adalah tulang punggung dari *World Wide Web*, memungkinkan pertukaran informasi antara klien (seperti *browser web*) dan *server*. Versi awal HTTP dirancang sebagai protokol sederhana untuk mengambil file dan dokumen

berbasis teks dari server ke pengguna. Namun, dengan berkembangnya teknologi, HTTP telah berkembang menjadi protokol yang mendukung berbagai format data, seperti gambar, video, dan API berbasis JSON.

HTTPS (*HTTP Secure*) adalah versi aman dari HTTP yang menggunakan *Transport Layer Security* (TLS) untuk mengenkripsi komunikasi antara klien dan *server*. HTTPS memastikan integritas data, otentikasi, dan kerahasiaan informasi, menjadikannya protokol utama untuk aplikasi yang membutuhkan keamanan tinggi, seperti *e-commerce*, perbankan, dan IoT.

6.4.1 Arsitektur HTTP/HTTPS

HTTP/HTTPS menggunakan arsitektur *client-server* di mana klien mengirimkan permintaan (*request*) ke *server*, dan *server* memberikan tanggapan (*response*) sesuai dengan permintaan tersebut. Protokol ini menggunakan model komunikasi *request-response* berbasis koneksi *stateless*, yang berarti setiap permintaan diproses secara independen tanpa menyimpan informasi dari permintaan sebelumnya.

6.4.2 Komponen Utama HTTP/HTTPS

Klien (*Client*):

Perangkat atau aplikasi yang mengirimkan permintaan HTTP/HTTPS, seperti *browser web*, aplikasi seluler, atau perangkat IoT. Contoh: Google Chrome, Mozilla Firefox, atau aplikasi IoT berbasis REST API.

Server:

Perangkat atau sistem yang menerima permintaan dari klien dan mengirimkan respons. Contoh: Server web seperti Apache, Nginx, atau server berbasis cloud seperti AWS.

Resource (Sumber Daya):

Informasi atau file yang diminta oleh klien, seperti dokumen HTML, gambar, atau data API.

URI (*Uniform Resource Identifier*):

Alamat yang digunakan untuk mengidentifikasi sumber daya yang diminta. Format umum URI meliputi `http://www.example.com/resource`.

DAFTAR PUSTAKA

- Blanchette, J. C. and Merz, S. (eds) (2016) *Interactive Theorem Proving*. Cham: Springer International Publishing (Lecture Notes in Computer Science). doi: 10.1007/978-3-319-43144-4.
- Kordon, F. and Lemoine, M. (eds) (2004) *Formal Methods for Embedded Distributed Systems*. Boston, MA: Springer US. doi: 10.1007/b116264.
- Peters, M. A., Jandrić, P. and Hayes, S. (eds) (2022) *Bioinformational Philosophy and Postdigital Knowledge Ecologies*. Cham: Springer International Publishing (Postdigital Science and Education). doi: 10.1007/978-3-030-95006-4.
- Sultan, M. *et al.* (eds) (2022) *Energy Systems and Applications in Agriculture*. MDPI. doi: 10.3390/books978-3-0365-5007-7.
- Tavasszy, L. and Piecyk, M. (2018) 'Sustainable Freight Transport', *Sustainability*, 10(10), p. 3624. doi: 10.3390/su10103624.
- Tennina, S. *et al.* (2013) *IEEE 802.15.4 and ZigBee as Enabling Technologies for Low-Power Wireless Systems with Quality-of-Service Constraints*. Berlin, Heidelberg: Springer Berlin Heidelberg (SpringerBriefs in Electrical and Computer Engineering). doi: 10.1007/978-3-642-37368-8.
- Tsai, W.-H. (2019) 'Modelling and Analysis of Sustainability Related Issues in New Era', *Sustainability*, 11(7), p. 2134. doi: 10.3390/su11072134.

BAB 7

KEAMANAN IoT

Oleh Yendi Putra

7.1 Pendahuluan

Internet of Things (IoT) telah mengubah cara manusia berinteraksi dengan teknologi, memungkinkan perangkat untuk saling terhubung dan berkomunikasi secara otomatis tanpa intervensi langsung dari pengguna. Dari rumah pintar, kendaraan otonom, hingga sistem industri yang dikendalikan jarak jauh, IoT telah menjadi bagian tak terpisahkan dari kehidupan modern. Namun, di balik kenyamanan dan efisiensi yang ditawarkan, IoT juga menghadirkan tantangan besar dalam hal keamanan. Perangkat yang terkoneksi ke internet berpotensi menjadi pintu masuk bagi peretas untuk mengeksploitasi celah keamanan, mencuri data pribadi, atau bahkan mengendalikan perangkat tanpa izin. Dengan semakin banyaknya perangkat IoT yang digunakan di berbagai sektor, ancaman terhadap keamanan digital semakin meningkat, menuntut solusi yang efektif dan berkelanjutan.



Gambar 7. 1 Ilustrasi IoT

Keamanan dalam IoT menjadi perhatian utama karena perangkat yang digunakan sering kali memiliki sistem keamanan yang lemah. Banyak perangkat IoT dibuat dengan keterbatasan daya komputasi dan sumber daya, sehingga produsen sering kali mengabaikan penerapan protokol keamanan yang ketat. Selain itu, tidak semua perangkat IoT mendapatkan pembaruan perangkat lunak secara berkala, yang membuatnya rentan terhadap eksploitasi oleh penyerang. Serangan terhadap IoT tidak hanya berdampak pada perangkat itu sendiri tetapi juga dapat membahayakan infrastruktur yang lebih luas, seperti jaringan listrik, rumah sakit, dan sistem transportasi. Oleh karena itu, pemahaman tentang ancaman keamanan IoT dan cara mitigasinya menjadi sangat penting bagi pengguna, pengembang, dan pemangku kepentingan lainnya.

Berbagai jenis serangan dapat terjadi pada perangkat IoT, mulai dari penyadapan komunikasi, pencurian data, serangan botnet, hingga pengambilalihan perangkat secara ilegal. Salah satu contoh serangan yang terkenal adalah serangan Mirai Botnet pada tahun 2016 (Mauliddiyah, 2021), di mana ribuan

perangkat IoT yang tidak diamankan dengan baik digunakan untuk meluncurkan serangan Distributed Denial of Service (DDoS) terbesar dalam sejarah. Serangan ini mengakibatkan gangguan besar pada layanan internet di berbagai negara. Studi kasus seperti ini menunjukkan betapa rentannya sistem IoT jika tidak dilindungi dengan baik. Oleh karena itu, buku ini akan mengulas berbagai kasus serangan yang telah terjadi, memberikan pemahaman tentang pola dan metode serangan, serta memberikan wawasan tentang bagaimana langkah-langkah keamanan dapat diterapkan untuk mencegah insiden serupa di masa depan.

Untuk mengatasi tantangan keamanan IoT, diperlukan pendekatan yang komprehensif dan berlapis. Langkah-langkah yang dapat diterapkan meliputi enkripsi data, otentikasi perangkat yang lebih ketat, pembaruan perangkat lunak yang rutin, serta implementasi *firewall* dan sistem deteksi intrusi. Selain itu, edukasi kepada pengguna juga menjadi faktor penting dalam meningkatkan keamanan IoT. Banyak serangan terjadi karena kelalaian pengguna dalam mengamankan perangkat mereka, seperti menggunakan kata sandi default atau menghubungkan perangkat ke jaringan yang tidak aman. Oleh karena itu, selain solusi teknis, kesadaran dan literasi digital juga menjadi bagian penting dalam strategi keamanan IoT yang efektif.

7.2 Pentingnya Keamanan Pada IoT

Keamanan dalam *Internet of Things* (IoT) menjadi aspek yang sangat krusial mengingat semakin banyaknya perangkat yang terhubung ke internet di berbagai sektor, mulai dari rumah tangga, industri, hingga pemerintahan. IoT memungkinkan perangkat untuk saling berkomunikasi dan bertukar data secara otomatis, tetapi tanpa langkah pengamanan yang memadai, perangkat-perangkat ini dapat menjadi celah bagi penyerang untuk mengeksploitasi sistem. Ancaman seperti pencurian data, penyadapan komunikasi, serta pengambilalihan kendali

perangkat oleh pihak yang tidak bertanggung jawab dapat menimbulkan dampak yang signifikan. Misalnya, dalam konteks rumah pintar, peretasan pada perangkat seperti kamera pengawas atau kunci pintar dapat membahayakan privasi dan keamanan penggunanya. Sementara itu, di sektor industri, serangan terhadap sistem IoT dapat mengganggu operasional perusahaan, menyebabkan kerugian finansial yang besar, serta membahayakan keselamatan pekerja jika sistem yang dikendalikan secara otomatis mengalami gangguan atau manipulasi.

Selain ancaman langsung terhadap individu dan industri, keamanan IoT juga memiliki dampak yang lebih luas terhadap infrastruktur digital secara keseluruhan. Salah satu ancaman terbesar yang dihadapi dalam ekosistem IoT adalah serangan botnet, di mana ribuan atau bahkan jutaan perangkat IoT yang tidak diamankan dengan baik digunakan oleh peretas untuk melancarkan serangan siber berskala besar. Contoh nyata dari serangan ini adalah serangan Mirai Botnet pada tahun 2016 yang memanfaatkan kelemahan keamanan pada perangkat IoT untuk melumpuhkan layanan internet di berbagai negara. Serangan semacam ini menunjukkan bahwa perangkat IoT yang tidak dilindungi tidak hanya berisiko bagi pemiliknya, tetapi juga dapat digunakan untuk menyerang sistem lain, menciptakan ancaman yang lebih luas terhadap jaringan global. Oleh karena itu, keamanan dalam IoT bukan hanya tanggung jawab individu atau organisasi tertentu, tetapi juga menjadi perhatian kolektif yang harus dikelola dengan pendekatan yang komprehensif dan berkelanjutan.

Untuk mengatasi risiko keamanan dalam IoT, diperlukan penerapan berbagai strategi pengamanan yang mencakup aspek teknis, regulasi, serta kesadaran pengguna. Dari sisi teknis, produsen perangkat IoT harus memastikan bahwa produk mereka dilengkapi dengan fitur keamanan seperti enkripsi data, autentikasi yang kuat, serta pembaruan perangkat lunak secara berkala. Regulasi juga memainkan peran penting dalam memastikan standar keamanan diterapkan oleh industri, sehingga perangkat yang beredar di pasaran memiliki perlindungan yang memadai. Selain itu, kesadaran pengguna

juga harus ditingkatkan agar mereka memahami pentingnya mengamankan perangkat IoT yang mereka gunakan, seperti mengganti kata sandi default, menghindari jaringan yang tidak aman, dan rutin memperbarui firmware. Dengan kombinasi upaya dari berbagai pihak, keamanan dalam ekosistem IoT dapat ditingkatkan, sehingga manfaat dari teknologi ini dapat dinikmati tanpa mengorbankan aspek keselamatan dan privasi.

7.3 Regulasi dan Standar Keamanan IoT

Regulasi dan standar keamanan dalam Internet of Things (IoT) menjadi aspek krusial dalam menjaga ekosistem digital yang aman dan andal. Seiring dengan meningkatnya jumlah perangkat IoT yang digunakan di berbagai sektor, ancaman keamanan juga semakin kompleks, sehingga diperlukan regulasi yang jelas untuk memastikan bahwa perangkat-perangkat tersebut memiliki proteksi yang memadai. Beberapa negara dan organisasi internasional telah mengembangkan standar keamanan untuk IoT guna melindungi data pengguna dan mencegah potensi serangan siber. Misalnya, *General Data Protection Regulation* (GDPR) di Uni Eropa mengatur perlindungan data pribadi pengguna IoT, sedangkan *California Consumer Privacy Act* (CCPA) di Amerika Serikat mewajibkan produsen perangkat IoT untuk menerapkan langkah-langkah keamanan yang memadai (Marikyan et al., 2021). Di tingkat global, *International Organization for Standardization* (ISO) dan *National Institute of Standards and Technology* (NIST) telah menetapkan pedoman teknis untuk meningkatkan keamanan perangkat dan jaringan IoT.



Gambar 7. 2 GDPR

Sumber: <https://theconversation.com/>

1. *International Organization for Standardization (ISO)*

ISO telah menetapkan beberapa standar untuk meningkatkan keamanan perangkat dan jaringan IoT, antara lain:

- a. ISO/IEC 27001 – Standar Manajemen Keamanan Informasi
 - Mengatur pengelolaan risiko keamanan informasi dalam sistem IoT.
 - Mewajibkan perlindungan data dengan enkripsi dan kontrol akses.
 - Menetapkan kebijakan keamanan untuk mencegah serangan siber (Culot et al., 2021).
- b. ISO/IEC 27002 – Pedoman Praktik Keamanan Informasi
 - Menyediakan panduan implementasi kontrol keamanan untuk perangkat IoT.
 - Mengatur pemantauan, deteksi, dan respons terhadap ancaman keamanan.

- Menekankan pentingnya pelatihan dan kesadaran pengguna terhadap keamanan IoT (Erlangung & Master, 2023).
- c. ISO/IEC 29147 – Pengungkapan Kerentanan Keamanan
 - Mengatur cara menangani laporan celah keamanan pada perangkat IoT.
 - Mewajibkan transparansi dalam perbaikan bug dan pembaruan keamanan.
 - Memberikan pedoman komunikasi kepada pengguna mengenai risiko keamanan (Polemi, n.d.).
- d. ISO/IEC 15408 (*Common Criteria*) – Evaluasi Keamanan Teknologi Informasi
 - Mengatur metode evaluasi keamanan perangkat IoT sebelum digunakan.
 - Memastikan bahwa perangkat memenuhi persyaratan keamanan yang ketat.
 - Digunakan dalam sertifikasi keamanan produk teknologi, termasuk IoT (Dotsenko et al., 2019).

2. ***National Institute of Standards and Technology (NIST)***

NIST memberikan pedoman teknis untuk meningkatkan keamanan IoT melalui beberapa standar berikut (Guston, 2012):

- a. NIST *Special Publication* (SP) 800-183 – Panduan Keamanan IoT
 - Memberikan kerangka kerja keamanan untuk sistem berbasis IoT.
 - Menekankan pentingnya enkripsi, autentikasi, dan segmentasi jaringan.
 - Mewajibkan pemantauan dan pemeliharaan perangkat IoT secara berkala.
- b. NIST *Cybersecurity Framework* (CSF) – Kerangka Kerja Keamanan Siber
 - Menyediakan pendekatan berbasis risiko untuk melindungi ekosistem IoT.
 - Mengatur lima fungsi utama: Identify, Protect, Detect, Respond, Recover.

- Digunakan oleh organisasi untuk mengembangkan strategi keamanan IoT.
- c. NIST SP 800-193 – Keamanan Perangkat Keras IoT
 - Menetapkan standar keamanan untuk *firmware* dan perangkat keras IoT.
 - Mengatur metode proteksi terhadap serangan berbasis perangkat keras.
 - Memastikan adanya mekanisme pemulihan jika terjadi kompromi sistem.
- d. NIST SP 800-53 – Pengamanan Sistem Informasi Federal
 - Mewajibkan perangkat IoT yang digunakan dalam sistem pemerintah memiliki keamanan tingkat tinggi.
 - Mengatur kebijakan akses berbasis peran (*role-based access control*) untuk mencegah akses yang tidak sah.
 - Memastikan perangkat IoT memenuhi persyaratan enkripsi komunikasi yang aman.

Meskipun berbagai regulasi dan standar telah dibuat, tantangan dalam implementasinya tetap besar. Salah satu kendala utama adalah kurangnya keseragaman dalam standar keamanan, karena setiap negara memiliki kebijakan yang berbeda terkait IoT. Hal ini menyebabkan perbedaan dalam cara produsen menerapkan langkah-langkah keamanan, yang pada akhirnya dapat menciptakan celah bagi peretas untuk mengeksploitasi sistem yang kurang terlindungi. Selain itu, banyak produsen IoT yang lebih mengutamakan fitur dan harga murah daripada aspek keamanan, sehingga mereka sering kali mengabaikan penerapan enkripsi, autentikasi yang kuat, atau pembaruan perangkat lunak secara berkala. Di sisi lain, pengguna juga sering kali tidak memahami pentingnya standar keamanan ini, sehingga mereka menggunakan perangkat tanpa konfigurasi yang benar, membuatnya rentan terhadap serangan siber.

Untuk memastikan regulasi dan standar keamanan IoT dapat diterapkan secara efektif, dibutuhkan kerja sama antara pemerintah, industri, dan masyarakat. Pemerintah harus

mengeluarkan kebijakan yang lebih ketat serta menegakkan kepatuhan terhadap standar keamanan yang ada. Sementara itu, industri harus lebih proaktif dalam mengembangkan perangkat yang memiliki keamanan bawaan (*security by design*) dan memastikan adanya pembaruan perangkat lunak secara berkala. Di sisi pengguna, edukasi mengenai praktik keamanan IoT, seperti penggunaan kata sandi yang kuat dan pembaruan perangkat lunak secara rutin, harus terus ditingkatkan. Dengan adanya regulasi dan standar yang jelas serta kesadaran yang lebih tinggi dari semua pihak, ancaman keamanan dalam IoT dapat diminimalkan, sehingga teknologi ini dapat terus berkembang dengan lebih aman dan memberikan manfaat yang maksimal bagi masyarakat.

7.4 Kasus-kasus Serangan Pada IOT

Seiring meningkatnya penggunaan perangkat IoT di berbagai sektor, serangan siber terhadap sistem ini juga semakin sering terjadi. Berikut adalah beberapa kasus serangan IoT yang telah terjadi secara global, termasuk kronologi, data waktu dan lokasi, serta jenis serangan dan dampaknya (Rafsanjani et al., 2022) (Sari et al., 2023).

Tabel 7. 1 Kasus-kasus Serangan Pada IoT

No	Nama Serangan	Kronologi Serangan	Waktu dan Lokasi	Jenis Serangan	Dampak
1	Mirai Botnet	Malware Mirai menginfeksi perangkat IoT dengan kredensial default dan menggunakannya untuk serangan DDoS besar-besaran.	21 Oktober 2016, Global (terutama AS dan Eropa)	Serangan DDoS	Mengganggu layanan besar seperti Twitter, Netflix, dan Reddit.
2	Stuxnet	Worm yang dirancang untuk menyerang	2010, Iran	Eksplorasi perangkat IoT	Merusak program nuklir Iran dengan

No	Nama Serangan	Kronologi Serangan	Waktu dan Lokasi	Jenis Serangan	Dampak
		sistem SCADA di fasilitas nuklir Iran melalui perangkat IoT yang dikompromikan.		industri	mengganggu sentrifugal uranium.
3	BrickerBot	Malware yang merusak perangkat IoT dengan menghapus firmware, membuatnya tidak dapat digunakan.	2017, Global	Permanen Denial-of-Service (DDoS)	Ribuan perangkat IoT tidak dapat diperbaiki setelah terinfeksi.
4	Serangan Target (HVAC IoT Breach)	Peretas masuk melalui sistem kontrol HVAC IoT dan mencuri data kartu kredit pelanggan.	2013, AS	Penyusupan jaringan melalui IoT	40 juta data kartu kredit pelanggan dicuri.
5	Serangan Jeep Cherokee	Peretas mengambil alih sistem kendaraan Jeep Cherokee melalui eksploitasi jaringan IoT dalam mobil.	2015, AS	Remote Code Execution (RCE) pada IoT kendaraan	Kendaraan dapat dikendalikan dari jarak jauh, membahayakan pengemudi.
6	Serangan pada Kamera IoT Verkada	Hacker membobol sistem kamera pengawas Verkada dan mengakses rekaman di	Maret 2021, Global	Pelanggaran privasi melalui akses ilegal ke IoT	Ribuan rekaman di rumah sakit, sekolah, dan kantor terekspos.

No	Nama Serangan	Kronologi Serangan	Waktu dan Lokasi	Jenis Serangan	Dampak
		berbagai institusi.			
7	Serangan pada Infrastruktur Listrik Ukraina	Peretas menggunakan malware IoT untuk mengganggu distribusi listrik di Ukraina.	Desember 2015, Ukraina	Serangan siber terhadap infrastruktur kritis	Listrik padam di berbagai wilayah Ukraina selama berjam-jam.

Dari kasus di atas menunjukkan kompleksitas tantangan keamanan yang dihadapi oleh ekosistem IoT dan pentingnya untuk terus memperbarui, mengamankan, dan memantau perangkat IoT agar terhindar dari serangan.

7.5 Jenis-jenis Serangan Pada IoT

Dalam ekosistem *Internet of Things* (IoT), perangkat yang saling terhubung menjadi target utama bagi berbagai jenis ancaman siber. Berikut ini adalah beberapa bentuk serangan yang sering terjadi pada perangkat IoT:

7.5.1 Serangan DDoS (*Distributed Denial of Service*)

Serangan DDoS terjadi ketika sejumlah besar permintaan dikirim secara bersamaan ke suatu perangkat atau jaringan, dengan tujuan membebani sumber daya hingga tidak dapat beroperasi secara normal. Pada IoT, perangkat yang memiliki keamanan lemah dapat diambil alih oleh botnet dan digunakan untuk meluncurkan serangan ini, seperti yang terjadi pada serangan Mirai Botnet yang melumpuhkan banyak layanan internet di seluruh dunia (Maulidiyah, 2021).

7.5.2 *Man-in-the-Middle Attack (MitM)*

Dalam serangan ini, peretas menyusup di antara komunikasi dua perangkat IoT tanpa diketahui oleh kedua pihak yang berkomunikasi. Mereka dapat mencuri, mengubah, atau menyisipkan data berbahaya dalam transmisi tersebut. Kelemahan dalam enkripsi atau autentikasi menjadi faktor utama yang memungkinkan serangan ini terjadi.

7.5.3 *Malware dan Ransomware pada IoT*

Malware adalah perangkat lunak berbahaya yang dirancang untuk menyusup, mencuri data, atau merusak sistem pada perangkat IoT. Sementara itu, *ransomware* mengenkripsi data pengguna dan menuntut pembayaran tebusan agar akses dapat dikembalikan. Karena IoT sering kali memiliki sistem keamanan yang terbatas, *malware* dan *ransomware* dapat dengan mudah menyebar melalui jaringan yang kurang terlindungi.

7.5.4 Serangan Fisik terhadap Perangkat IoT

Perangkat IoT yang ditempatkan di lokasi terbuka berisiko mengalami gangguan fisik. Serangan ini bisa berupa pencurian, kerusakan perangkat, hingga manipulasi perangkat keras untuk mengakses informasi sensitif atau menyisipkan kode berbahaya. Keamanan fisik seperti penguncian perangkat dan sistem deteksi gangguan sangat diperlukan untuk mencegah ancaman ini.

7.5.5 Serangan pada Protokol Komunikasi IoT

Protokol komunikasi yang digunakan dalam IoT, seperti MQTT, CoAP, atau Zigbee, sering kali memiliki celah keamanan yang dapat dieksploitasi oleh peretas. Jika tidak dikonfigurasi dengan baik, protokol ini dapat digunakan untuk mengakses dan mengendalikan perangkat IoT secara

ilegal, menyebabkan kebocoran data atau gangguan operasional.

7.5.6 Eksploitasi *Firmware* dan *Hardware*

Firmware adalah perangkat lunak yang mengontrol fungsi dasar perangkat IoT. Jika *firmware* tidak diperbarui atau memiliki kelemahan keamanan, peretas dapat mengeksploitasinya untuk mendapatkan akses tidak sah. Selain itu, eksploitasi pada komponen perangkat keras dapat memungkinkan penyerang mengubah fungsi perangkat atau menyisipkan backdoor untuk akses lebih lanjut.

Serangan-serangan ini menunjukkan bahwa keamanan IoT harus menjadi prioritas utama dalam pengembangan dan penerapannya. Dengan menerapkan enkripsi yang kuat, memperbarui *firmware* secara berkala, serta meningkatkan sistem keamanan fisik dan jaringan, risiko serangan terhadap perangkat IoT dapat diminimalkan.

7.6 Penanganan Dan Strategi Keamanan IOT

Seiring dengan semakin luasnya adopsi *Internet of Things* (IoT) dalam berbagai sektor, tantangan keamanan menjadi semakin kompleks. Perangkat IoT yang saling terhubung rentan terhadap berbagai jenis serangan siber, mulai dari pencurian data hingga eksploitasi sistem untuk kepentingan jahat. Oleh karena itu, diperlukan strategi yang komprehensif dalam mendeteksi, mencegah, dan menangani ancaman terhadap ekosistem IoT. Bagian ini akan membahas berbagai metode penanganan dan strategi keamanan yang dapat diterapkan untuk melindungi perangkat IoT dari risiko serangan, memastikan integritas data, serta menjaga keandalan sistem secara keseluruhan diantaranya sebagai berikut:

7.6.1 Metode Deteksi dan Pencegahan Serangan IoT

Keamanan perangkat IoT memerlukan pendekatan yang komprehensif untuk mendeteksi dan mencegah serangan siber. Salah satu metode utama adalah pemantauan lalu lintas jaringan secara real-time, yang dapat dilakukan dengan menerapkan *Intrusion Detection System* (IDS) dan *Intrusion Prevention System* (IPS). IDS bertugas mengidentifikasi pola serangan dengan menganalisis anomali dalam lalu lintas data, sedangkan IPS bertindak dengan segera untuk mencegah ancaman sebelum berdampak lebih jauh. Selain itu, penggunaan kecerdasan buatan dalam analisis lalu lintas jaringan memungkinkan sistem mendeteksi serangan yang belum pernah diketahui sebelumnya, sehingga memberikan perlindungan lebih kuat terhadap perangkat IoT.

Selain pemantauan jaringan, penggunaan autentikasi berlapis dan enkripsi data sangat penting dalam mencegah akses tidak sah ke perangkat IoT. Autentikasi dua faktor (2FA) dapat meningkatkan perlindungan akses pengguna, sementara enkripsi data menggunakan *Transport Layer Security* (TLS) dan *Virtual Private Network* (VPN) memastikan bahwa komunikasi antar perangkat tetap aman dari penyadapan. Pengguna juga harus menghindari penggunaan kata sandi default dan menggantinya dengan kredensial unik untuk setiap perangkat (Syahputri et al., 2023). Selain itu, segmentasi jaringan dengan cara memisahkan perangkat IoT dari jaringan utama dapat membatasi dampak serangan jika salah satu perangkat berhasil diretas.

Pembaruan sistem secara berkala dan peningkatan kesadaran pengguna juga berperan besar dalam mencegah serangan pada IoT. Banyak serangan terjadi akibat kelemahan dalam *firmware* yang tidak diperbarui, sehingga produsen dan pengguna harus rutin melakukan update keamanan agar sistem tetap terlindungi dari eksploitasi

terbaru. Selain itu, edukasi dan pelatihan kepada pengguna mengenai ancaman siber serta praktik terbaik dalam menggunakan IoT dapat membantu mengurangi risiko serangan. Dengan menggabungkan pemantauan jaringan, autentikasi yang kuat, enkripsi data, pembaruan sistem, serta kesadaran pengguna, perangkat IoT dapat lebih aman dari berbagai ancaman siber.

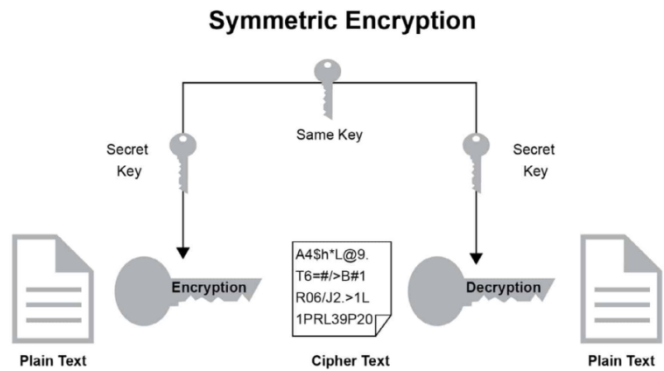
7.6.2 Enkripsi dan Keamanan Data pada IoT

Enkripsi adalah proses mengubah informasi atau data menjadi bentuk yang tidak dapat dibaca atau dipahami tanpa menggunakan kunci khusus. Tujuan utama enkripsi adalah untuk melindungi data dari akses yang tidak sah, sehingga hanya pihak yang memiliki kunci dekripsi yang dapat mengembalikan data ke bentuk aslinya.

Enkripsi dapat dibagi menjadi dua jenis utama berdasarkan penggunaan kunci:

1. Enkripsi Simetris

Enkripsi simetris adalah metode kriptografi yang menggunakan satu kunci yang sama untuk proses enkripsi dan dekripsi. Artinya, kunci yang digunakan untuk mengubah data asli (*plaintext*) menjadi data terenkripsi (*ciphertext*) juga digunakan untuk mengembalikan data tersebut ke bentuk aslinya.



Gambar 8. 1 Enkripsi Simetris

Cara Kerja Enkripsi Simetris

1. Pengguna menginput data yang akan dienkrpsi.
2. Algoritma enkripsi mengubah data tersebut menjadi *ciphertext* menggunakan kunci enkripsi yang telah ditentukan.
3. Penerima yang memiliki kunci yang sama dapat mendekripsi *ciphertext* kembali menjadi data asli.

2. ***Advanced Encryption Standard (AES)***

Advanced Encryption Standard (AES) merupakan salah satu algoritma kriptografi yang paling banyak digunakan untuk melindungi data dalam berbagai sistem, termasuk pada perangkat *Internet of Things (IoT)*. Teknik ini bekerja dengan cara mengubah informasi asli menjadi format terenkripsi yang sulit dipahami tanpa kunci dekripsi yang valid. AES dikembangkan sebagai pengganti *Data Encryption Standard (DES)* karena memiliki tingkat keamanan yang lebih tinggi serta efisiensi dalam pemrosesan data. AES memiliki Karakteristik sebagai berikut (Putra et al., 2021):

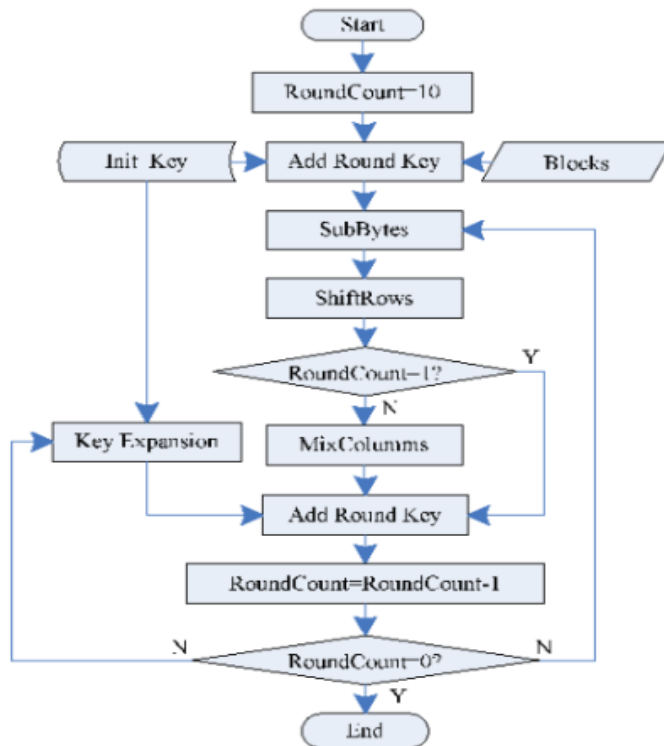
1. Struktur Enkripsi Blok

AES merupakan algoritma enkripsi berbasis blok yang memproses data dalam ukuran tetap, yaitu 128-bit per blok. Blok data ini kemudian mengalami beberapa tahapan transformasi, termasuk substitusi, pergantian posisi, dan pencampuran untuk meningkatkan keamanan.

2. **Ukuran Kunci yang Fleksibel**
AES mendukung tiga ukuran kunci enkripsi, yaitu 128-bit, 192-bit, dan 256-bit. Semakin besar ukuran kunci, semakin sulit sistem untuk diretas karena jumlah kombinasi yang harus dicoba oleh penyerang menjadi jauh lebih banyak.
3. **Jumlah Putaran Berbeda Berdasarkan Panjang Kunci**
4. **Proses enkripsi dalam AES dilakukan dalam beberapa putaran (rounds) tergantung pada panjang kunci yang digunakan:**
 - 10 putaran pada kunci 128-bit
 - 12 putaran pada kunci 192-bit
 - 14 putaran pada kunci 256-bitSetiap putaran mencakup operasi substitusi byte, pergeseran baris, pencampuran kolom, dan penambahan kunci.
5. **Kecepatan dan Efisiensi**
AES dikenal memiliki performa yang cepat dan efisien dalam pemrosesan data, baik dalam perangkat lunak maupun perangkat keras. Oleh karena itu, AES sering digunakan dalam IoT yang memiliki keterbatasan sumber daya komputasi.
6. **Keamanan yang Tinggi**
Hingga saat ini, AES dianggap sangat aman dan belum pernah ditembus oleh serangan brute force dalam kondisi normal. Kombinasi antara panjang kunci yang besar dan kompleksitas algoritma

membuatnya sangat sulit untuk diretas dengan metode komputasi konvensional.

Proses enkripsi AES terdiri dari serangkaian operasi yang diulang pada setiap putaran dapat di lihat pada gambar dibawah ini:



Gambar 7.3 Algoritma AES

Penjelasnya dari gambar adalah

1. *SubBytes*: Operasi substitusi di mana setiap byte digantikan dengan byte lain sesuai dengan tabel substitusi yang disebut S-box.
2. *ShiftRows*: Operasi penggeseran di mana baris-baris dalam blok 4x4 byte dirotasi ke kiri dengan jumlah tertentu.

3. *MixColumns*: Operasi permutasi di mana setiap kolom dalam blok di-multiplikasi dengan matriks tetap.
4. *AddRoundKey*: Setiap byte dari blok XOR dengan kunci putaran yang dihasilkan dari kunci asli menggunakan algoritma penjadwalan kunci (Andriani et al., 2019).

3. Penerapan AES dalam IoT

Dalam IoT, AES digunakan untuk mengamankan komunikasi antarperangkat dan melindungi data yang tersimpan dari akses tidak sah. Dengan menerapkan AES, informasi yang dikirim melalui jaringan IoT menjadi lebih sulit untuk disadap atau dimodifikasi oleh pihak yang tidak berwenang. Selain itu, algoritma ini juga dapat digunakan bersama metode keamanan lainnya, seperti autentikasi dan manajemen kunci yang baik, guna meningkatkan perlindungan terhadap berbagai ancaman siber.

Berikut adalah tabel yang menyajikan keunggulan dan kelemahan enkripsi simetris:

Tabel 7. 2 Keunggulan dan Kelemahan Enkripsi Simetris

Keunggulan	Kelemahan
Kecepatan tinggi – Proses enkripsi dan dekripsi lebih cepat dibandingkan enkripsi asimetris karena algoritmanya lebih sederhana.	Distribusi kunci yang rentan – Kunci harus dibagikan ke pihak yang berwenang, dan jika tidak dikelola dengan baik, bisa disalahgunakan.
Efisiensi dalam pengolahan data – Cocok untuk mengamankan data dalam jumlah besar dengan sumber daya komputasi yang lebih sedikit.	Kurang aman dibandingkan enkripsi asimetris – Jika kunci diketahui oleh pihak yang tidak berwenang, seluruh data yang terenkripsi bisa diakses.
Lebih mudah diimplementasikan –	Tidak mendukung autentikasi digital – Enkripsi simetris

Keunggulan	Kelemahan
Algoritmanya lebih sederhana dibandingkan enkripsi asimetris, sehingga lebih mudah diterapkan dalam berbagai sistem.	tidak menyediakan tanda tangan digital, sehingga sulit untuk memverifikasi identitas pengirim data.
Hemat daya dan sumber daya – Memerlukan lebih sedikit kapasitas penyimpanan dan daya komputasi dibandingkan enkripsi asimetris.	Tidak cocok untuk komunikasi skala besar – Karena setiap pasangan pengguna membutuhkan kunci unik, pengelolaan kunci menjadi lebih sulit dalam sistem yang memiliki banyak pengguna.

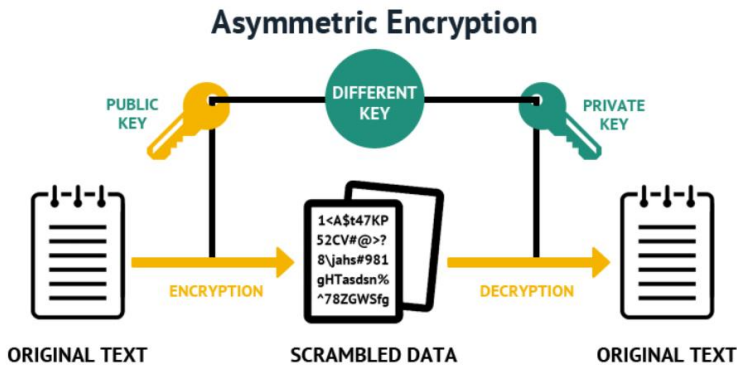
Tabel diatas menggambarkan bahwa meskipun enkripsi simetris sangat cepat dan efisien, kelemahan utama terletak pada keamanan distribusi kunci dan skalabilitas dalam sistem besar. Karena hanya satu kunci yang digunakan, keamanan data sangat bergantung pada bagaimana kunci tersebut disimpan dan dikirimkan. Jika kunci jatuh ke tangan yang tidak berwenang, maka keamanan sistem dapat terancam.

4. Enkripsi Asimetris

Enkripsi asimetris adalah metode kriptografi yang menggunakan dua kunci berbeda, yaitu kunci publik untuk enkripsi dan kunci privat untuk dekripsi. Artinya, data yang dienkripsi dengan kunci publik hanya dapat didekripsi menggunakan kunci privat yang sesuai. Metode ini meningkatkan keamanan karena kunci privat tidak perlu dibagikan kepada siapa pun. Cara Kerja Enkripsi Asimetris (Saputro et al., 2020)

1. Pihak pengirim mengenkripsi data menggunakan kunci publik penerima.
2. Data yang telah dienkripsi (*ciphertext*) dikirimkan melalui jaringan.

3. Penerima mendekripsi data menggunakan kunci privat yang hanya dimiliki olehnya.
4. Pesan asli (*plaintext*) berhasil diakses dengan aman tanpa risiko kunci bocor selama proses transmisi.



Gambar 7. 4 Enkripsi Asimetris

5. RSA (*Rivest-Shamir-Adleman*)

Algoritma RSA (*Rivest-Shamir-Adleman*) merupakan salah satu metode kriptografi kunci publik yang paling populer dan sering digunakan. RSA berfungsi untuk proses enkripsi, dekripsi, serta tanda tangan digital. Algoritma ini didasarkan pada kesulitan faktorisasi bilangan besar, di mana keamanannya terletak pada kompleksitas memfaktorkan hasil perkalian dua bilangan prima besar (Agustina et al., 2017).

Tahapan Algoritma RSA

a. Pembuatan Kunci

1. Menghitung n sebagai hasil perkalian p dan q :

$$n = p \times q$$
 - n digunakan untuk modulus pada kunci publik dan kunci privat.
2. Menghitung fungsi totient Euler, $\phi(n)$:

$$\phi(n) = (p-1) \times (q-1)$$

- $\phi(n)$ adalah jumlah bilangan bulat positif yang lebih kecil dari n dan relatif prima terhadap n .
- 3. Pilih bilangan bulat e (eksponen publik):
 - e harus memenuhi $1 < e < \phi(n)$ dan $\gcd(e, \phi(n)) = 1$.
- 4. Hitung d (eksponen privat):
 - d adalah invers modular dari e modulo $\phi(n)$, yaitu: $d \times e \equiv 1 \pmod{\phi(n)}$
- b. Kunci Publik dan Privat:
 - Kunci Publik: (e, n)
 - Kunci Privat: (d, n)
- c. Enkripsi:
 - Pesan *plaintext* M (harus dalam bentuk bilangan bulat yang lebih kecil dari n):
 $C = M^e \pmod{n}$ adalah ciphertext hasil enkripsi.
- d. Dekripsi:
 - *Ciphertext* C : $M = C^d \pmod{n}$
 - M adalah *plaintext* yang berhasil didekripsi.

RSA digunakan dalam berbagai sistem keamanan digital, termasuk komunikasi aman dan tanda tangan elektronik (Khamseyar & Basri, 2022). Berikut adalah perbandingan keunggulan dan kelemahan enkripsi asimetris dalam bentuk tabel:

Tabel 7.3 Keunggulan dan Kelemahan Enkripsi Asimetris

Aspek	Keunggulan	Kelemahan
Keamanan	Keamanan tinggi karena menggunakan dua kunci (publik & privat)	Rentan terhadap serangan <i>Man-in-the-Middle</i> jika kunci publik tidak

Aspek	Keunggulan	Kelemahan
		diverifikasi
Distribusi Kunci	Tidak perlu berbagi kunci rahasia, hanya kunci publik yang didistribusikan	Kunci publik bisa disalahgunakan jika tidak ada otoritas sertifikat yang valid
Otentikasi & Integritas	Mendukung tanda tangan digital untuk memastikan keaslian pesan	Memerlukan mekanisme tambahan untuk memastikan validitas kunci publik
Kecepatan & Efisiensi	Cocok untuk komunikasi terbuka di internet tanpa perlu kepercayaan awal	Lebih lambat dibandingkan enkripsi simetris karena proses perhitungan yang kompleks
Kinerja Komputasi	Digunakan untuk pertukaran kunci dalam protokol keamanan seperti SSL/TLS	Membutuhkan lebih banyak daya pemrosesan dan memori
Ukuran Data	Bisa digunakan untuk mengenkripsi pesan pendek dengan aman	Hasil enkripsi lebih besar dibandingkan enkripsi simetris, kurang efisien untuk file besar

7.6.3 Keamanan Jaringan IoT

Keamanan jaringan dalam ekosistem Internet of Things (IoT) menjadi aspek yang sangat penting karena perangkat IoT terus berkomunikasi dan saling bertukar data melalui jaringan. Tanpa sistem perlindungan yang memadai, jaringan IoT rentan terhadap berbagai ancaman siber seperti peretasan, penyadapan data, serta serangan yang dapat mengganggu operasional perangkat. Oleh karena itu,

diperlukan strategi keamanan yang komprehensif untuk memastikan jaringan IoT tetap terlindungi dari ancaman eksternal maupun internal.

Ancaman terhadap Jaringan IoT

Jaringan IoT menghadapi berbagai risiko keamanan yang dapat membahayakan integritas data dan perangkat yang terhubung. Beberapa ancaman utama yang sering terjadi meliputi:

1. Serangan DDoS (*Distributed Denial of Service*) – Penyerang mengirimkan lalu lintas data dalam jumlah besar untuk membuat jaringan IoT menjadi tidak dapat diakses.
2. *Man-in-the-Middle Attack* (MitM) – Peretas menyusup di antara komunikasi perangkat IoT untuk menyadap atau memodifikasi data yang dikirim.
3. Eksploitasi Protokol Komunikasi – Celah keamanan pada protokol jaringan IoT dapat dimanfaatkan untuk mengakses atau mengontrol perangkat secara ilegal.
4. Pencurian Data dan Penyadapan – Informasi yang dikirim melalui jaringan dapat diakses oleh pihak yang tidak berwenang jika tidak dilindungi dengan baik.

Untuk mengatasi ancaman tersebut, berikut adalah beberapa langkah strategis dalam menjaga keamanan jaringan IoT:

1. Penerapan Enkripsi Data
Semua komunikasi dalam jaringan IoT harus dienkripsi agar informasi yang dikirim tidak mudah diakses oleh pihak yang tidak sah. Protokol keamanan seperti *Transport Layer Security* (TLS) dan AES (*Advanced Encryption Standard*) dapat digunakan untuk melindungi data selama proses transmisi.
2. Autentikasi dan Kontrol Akses
Menggunakan metode autentikasi berlapis seperti autentikasi dua faktor (2FA) dan sertifikat digital akan

memastikan hanya perangkat dan pengguna yang sah yang dapat mengakses jaringan IoT. Selain itu, sistem *Identity and Access Management* (IAM) dapat diterapkan untuk mengontrol hak akses berdasarkan tingkat keamanan yang dibutuhkan.

3. *Firewall* dan Sistem Deteksi Intrusi (IDS/IPS)
Memasang *firewall* serta sistem deteksi dan pencegahan intrusi (*Intrusion Detection System/Intrusion Prevention System* – IDS/IPS) akan membantu dalam mendeteksi serta mencegah serangan yang mencurigakan terhadap jaringan IoT.
4. Segmentasi Jaringan
Memisahkan jaringan IoT dari jaringan utama dengan menerapkan Virtual LAN (VLAN) atau *Network Segmentation* dapat mengurangi risiko penyebaran serangan jika satu perangkat IoT mengalami kompromi (Sutanto et al., 2011).
5. Pembaruan dan Pemeliharaan Keamanan Secara Berkala
Perangkat IoT harus selalu diperbarui dengan patch keamanan terbaru untuk mengatasi celah keamanan yang baru ditemukan. Selain itu, pemantauan jaringan secara berkala diperlukan untuk mendeteksi anomali yang mencurigakan.

Dengan menerapkan strategi keamanan yang tepat, jaringan IoT dapat terlindungi dari berbagai ancaman siber dan memastikan kelangsungan operasional perangkat yang terhubung tetap berjalan dengan aman dan efisien.

7.6.4 Manajemen Akses dan Autentikasi IoT

Manajemen akses dan autentikasi dalam *Internet of Things* (IoT) menjadi aspek penting dalam menjaga keamanan sistem, mengingat banyaknya perangkat yang saling terhubung dan bertukar data. Tanpa mekanisme autentikasi yang kuat, perangkat IoT rentan terhadap akses

tidak sah yang dapat menyebabkan pencurian data, penyusupan, hingga pengambilalihan kendali perangkat oleh pihak yang tidak berwenang. Oleh karena itu, penerapan sistem manajemen akses yang efektif sangat diperlukan untuk memastikan hanya entitas yang sah yang dapat mengakses dan mengontrol perangkat dalam jaringan IoT.

Manajemen Akses dalam IoT

Bertujuan untuk mengontrol hak akses pengguna dan perangkat terhadap data atau sumber daya dalam jaringan IoT. Beberapa strategi yang dapat diterapkan dalam manajemen akses meliputi:

1. *Role-Based Access Control* (RBAC) – Hak akses diberikan berdasarkan peran pengguna atau perangkat, misalnya administrator memiliki akses penuh, sementara pengguna biasa hanya memiliki akses terbatas (Ferraiolo et al., 1995).
2. *Attribute-Based Access Control* (ABAC) – Hak akses ditentukan berdasarkan atribut tertentu, seperti lokasi perangkat, jenis perangkat, atau waktu akses (Hu et al., 2014).
3. *Least Privilege Access* – Memberikan hak akses hanya sebatas yang dibutuhkan, guna meminimalkan risiko jika terjadi kebocoran keamanan.
4. *Zero Trust Architecture* (ZTA) – Tidak ada perangkat atau pengguna yang dianggap terpercaya secara otomatis, sehingga setiap akses harus melalui proses verifikasi yang ketat.
5. Manajemen Identitas dan Akses (IAM) – Menggunakan platform seperti *Identity and Access Management* (IAM) untuk mengelola identitas pengguna dan perangkat dalam sistem IoT.

Autentikasi dalam IoT

Autentikasi adalah proses verifikasi identitas pengguna atau perangkat sebelum diberikan akses ke suatu sistem. Dalam ekosistem IoT, metode autentikasi yang umum digunakan meliputi:

1. Autentikasi Berbasis Kata Sandi

Autentikasi berbasis kata sandi adalah metode keamanan yang paling umum digunakan untuk mengakses sistem, termasuk dalam ekosistem *Internet of Things* (IoT). Metode ini mengharuskan pengguna atau perangkat memasukkan kombinasi karakter tertentu, seperti huruf, angka, dan simbol, untuk membuktikan identitas mereka sebelum mendapatkan akses. Kata sandi bertindak sebagai kredensial utama yang digunakan untuk mengamankan perangkat IoT, aplikasi, dan layanan berbasis *cloud* yang terhubung dengan perangkat tersebut

2. Autentikasi Dua Faktor (2FA) atau *Multi-Factor Authentication* (MFA)

Metode keamanan yang mengharuskan pengguna untuk memberikan lebih dari satu bentuk verifikasi sebelum mendapatkan akses ke suatu sistem. Dalam ekosistem *Internet of Things* (IoT), penerapan autentikasi multi-faktor menjadi sangat penting untuk mencegah akses tidak sah terhadap perangkat dan data yang tersimpan di dalamnya.

Cara Kerja 2FA/MFA

Sistem 2FA menggabungkan dua lapisan keamanan, sedangkan MFA dapat mencakup tiga atau lebih faktor autentikasi. Faktor-faktor ini biasanya terdiri dari:

- 1) Sesuatu yang Diketahui – Kata sandi, PIN, atau pola yang hanya diketahui oleh pengguna.
- 2) Sesuatu yang Dimiliki – Perangkat fisik seperti *smartphone*, token keamanan, atau kartu pintar (*smart card*).

- 3) Sesuatu yang Melekat pada Pengguna – Identifikasi biometrik seperti sidik jari, pengenalan wajah, atau pemindaian retina.

Misalnya, jika seseorang ingin mengakses perangkat IoT yang dilindungi 2FA, mereka harus memasukkan kata sandi terlebih dahulu (faktor pertama) dan kemudian mengonfirmasi identitas mereka dengan kode OTP (*One-Time Password*) yang dikirim ke ponsel mereka (faktor kedua).

Sertifikat Digital dan Kriptografi Kunci Publik (PKI)

Sertifikat digital adalah dokumen elektronik yang digunakan untuk membuktikan identitas suatu perangkat, pengguna, atau layanan dalam jaringan IoT. Sertifikat ini dikeluarkan oleh *Certificate Authority* (CA), sebuah entitas terpercaya yang menjamin keabsahan identitas pemilik sertifikat (Aas et al., 2019).

Sertifikat digital biasanya berisi:

- 1) Kunci publik yang digunakan untuk enkripsi komunikasi.
- 2) Identitas pemilik sertifikat (misalnya, perangkat atau server IoT).
- 3) Tanda tangan digital dari CA, yang memastikan keaslian sertifikat.
- 4) Masa berlaku sertifikat, setelah itu harus diperbarui.

Dalam IoT, sertifikat digital digunakan untuk mengamankan komunikasi antar perangkat, sehingga hanya entitas yang memiliki sertifikat sah yang dapat bertukar data secara aman.

Autentikasi Berbasis Biometrik

Autentikasi berbasis biometrik adalah metode verifikasi identitas yang menggunakan karakteristik fisik atau perilaku individu sebagai faktor autentikasi. Dalam ekosistem *Internet of Things* (IoT), metode ini semakin

banyak digunakan untuk meningkatkan keamanan akses terhadap perangkat dan layanan, karena menawarkan tingkat keunikan dan keandalan yang lebih tinggi dibandingkan dengan kata sandi atau token fisik.

Autentikasi Berbasis Perangkat (*Device Authentication*).

Sebuah metode yang digunakan untuk memastikan bahwa hanya perangkat yang sah yang dapat mengakses jaringan atau sistem. Dalam ekosistem IoT, autentikasi perangkat menjadi penting karena banyak perangkat yang saling berkomunikasi tanpa campur tangan manusia. Oleh karena itu, diperlukan mekanisme yang dapat mengidentifikasi, memverifikasi, dan mengontrol akses perangkat secara otomatis guna mencegah ancaman keamanan seperti penyusupan atau peretasan.

Dengan menerapkan autentikasi yang kuat dan manajemen akses yang ketat, perangkat IoT dapat lebih terlindungi dari ancaman siber yang mengincar celah keamanan. Kombinasi antara kriptografi, kontrol hak akses yang tepat, serta pembaruan sistem secara berkala akan meningkatkan ketahanan ekosistem IoT terhadap serangan yang semakin canggih.

7.6.5 Framework Keamanan IoT

Tujuan untuk memberikan panduan dalam melindungi perangkat, jaringan, dan data dari serangan yang dapat mengganggu fungsionalitas sistem. *Framework* ini mencakup berbagai aspek keamanan, mulai dari autentikasi, enkripsi data, hingga manajemen akses dan pemantauan ancaman secara *real-time*.

Komponen Utama Framework Keamanan IoT

1. Keamanan Perangkat (*Device Security*)

Perangkat IoT sering kali memiliki keterbatasan dalam daya pemrosesan dan penyimpanan, sehingga perlu

dilengkapi dengan mekanisme keamanan yang efisien. Langkah-langkah yang dapat diterapkan termasuk penggunaan firmware yang diperbarui secara berkala, autentikasi perangkat sebelum mengakses jaringan, serta proteksi fisik untuk mencegah manipulasi langsung terhadap perangkat keras.

2. Keamanan Jaringan (*Network Security*)

Perangkat IoT terhubung melalui berbagai jenis jaringan, baik lokal maupun berbasis cloud. Untuk menjaga keamanan komunikasi antar perangkat, perlu diterapkan protokol enkripsi, seperti TLS (*Transport Layer Security*), serta segmentasi jaringan guna membatasi akses antar perangkat. Selain itu, penerapan *firewall* dan sistem deteksi intrusi (IDS/IPS) dapat membantu mencegah akses tidak sah ke dalam sistem.

3. Keamanan Data (*Data Security*)

Data yang dikirim dan disimpan dalam sistem IoT harus dilindungi agar tidak mudah diakses oleh pihak yang tidak berwenang. Salah satu metode yang digunakan adalah enkripsi data *end-to-end*, yang memastikan bahwa hanya penerima yang sah yang dapat membaca informasi tersebut. Selain itu, mekanisme integritas data, seperti tanda tangan digital, dapat diterapkan untuk mendeteksi manipulasi atau perubahan yang tidak sah pada data.

4. Manajemen Akses dan Identitas (IAM – *Identity and Access Management*)

Pengaturan hak akses yang ketat sangat penting dalam framework keamanan IoT. Penggunaan metode autentikasi ganda (2FA/MFA) serta manajemen sertifikat digital dapat memastikan bahwa hanya pengguna dan perangkat yang sah yang dapat mengakses sumber daya sistem. Dengan menerapkan

prinsip least privilege access, risiko eksploitasi akibat akses yang tidak terkendali dapat diminimalkan.

5. Pemantauan dan Deteksi Ancaman (*Threat Detection & Monitoring*)

Sistem IoT harus selalu dipantau untuk mendeteksi potensi ancaman sebelum terjadi serangan besar. Penerapan *Intrusion Detection Systems* (IDS) dan *Intrusion Prevention Systems* (IPS) dapat membantu dalam mengidentifikasi pola serangan yang mencurigakan. Selain itu, penggunaan kecerdasan buatan (AI) dan machine learning dalam analisis keamanan dapat meningkatkan efisiensi dalam mendeteksi ancaman secara otomatis.

7.7 Praktik Pengamanan IoT

7.7.1 Membangun Sistem Keamanan untuk Perangkat IoT

Dalam mengamankan IoT, langkah pertama yang harus dilakukan adalah membangun sistem keamanan yang kuat untuk perangkat yang terhubung ke jaringan. Karena perangkat IoT sering memiliki keterbatasan dalam daya pemrosesan dan kapasitas penyimpanan, strategi keamanan yang diterapkan harus efisien, ringan, namun tetap efektif dalam mencegah ancaman siber. beberapa langkah dalam membangun sistem keamanan IoT

1. Menggunakan Autentikasi yang Kuat

Setiap perangkat IoT harus dilengkapi dengan mekanisme autentikasi yang kuat sebelum dapat mengakses jaringan atau layanan tertentu. Metode seperti autentikasi dua faktor (2FA), penggunaan sertifikat digital, atau kriptografi kunci publik (PKI) dapat membantu mencegah akses tidak sah. Hindari penggunaan kata sandi default dan pastikan setiap perangkat memiliki kredensial unik.

2. Memastikan *Firmware* dan Perangkat Lunak Selalu Diperbarui
Perangkat IoT sering kali menjadi target serangan karena memiliki *firmware* yang usang dan rentan terhadap eksploitasi. Oleh karena itu, penting untuk menerapkan pembaruan perangkat lunak secara berkala dan memastikan bahwa setiap pembaruan berasal dari sumber resmi. Penerapan *Over-The-Air* (OTA) update dapat memudahkan proses pembaruan tanpa harus mengganti perangkat secara fisik.
3. Menggunakan Enkripsi untuk Melindungi Data
Data yang dikirim dan diterima oleh perangkat IoT harus dienkripsi agar tidak mudah diakses oleh pihak yang tidak berwenang. Penggunaan algoritma seperti *Advanced Encryption Standard* (AES) dan *Transport Layer Security* (TLS) dapat membantu melindungi informasi dari penyadapan dan manipulasi data.
4. Menerapkan Segmentasi Jaringan
Untuk mengurangi risiko penyebaran serangan, jaringan yang menghubungkan perangkat IoT sebaiknya dipisahkan dari jaringan utama perusahaan atau rumah. Penggunaan Virtual LAN (VLAN) atau jaringan khusus untuk IoT dapat membantu membatasi akses perangkat serta mencegah peretas mengeksploitasi satu perangkat untuk mengakses seluruh sistem.
5. Menambahkan Sistem Deteksi dan Pencegahan Ancaman
Memasang *Intrusion Detection System* (IDS) dan *Intrusion Prevention System* (IPS) di jaringan IoT memungkinkan sistem untuk mendeteksi serta menghentikan aktivitas mencurigakan secara otomatis. Selain itu, pemantauan berbasis kecerdasan buatan (AI) dapat meningkatkan deteksi terhadap ancaman

baru dengan mempelajari pola serangan yang pernah terjadi sebelumnya.

7.7.2 Konfigurasi Keamanan untuk *Router* dan *Gateway* IoT

Router dan *gateway* IoT berperan penting sebagai penghubung antara perangkat IoT dengan jaringan internet atau sistem internal. Oleh karena itu, konfigurasi keamanan yang tepat sangat diperlukan untuk mencegah akses tidak sah, penyadapan data, dan serangan siber lainnya. Berikut adalah dua konfigurasi keamanan utama yang dapat diterapkan.

1. Mengaktifkan *Firewall* dan Sistem Deteksi Intrusi (IDS/IPS)

Firewall dan *Intrusion Detection System* (IDS)/*Intrusion Prevention System* (IPS) adalah komponen penting dalam perlindungan *router* dan *gateway* IoT.

Konfigurasi *Firewall*:

- Blokir lalu lintas tidak dikenal: Konfigurasi *firewall* untuk hanya mengizinkan lalu lintas dari sumber yang terpercaya dan memblokir koneksi masuk dari alamat IP yang mencurigakan.
- Gunakan aturan berbasis *whitelist*: Hanya perangkat yang terdaftar yang diizinkan untuk terhubung ke jaringan.
- Batasi akses ke *port* penting: Tutup atau nonaktifkan port yang tidak digunakan (misalnya Telnet, SSH, HTTP jika tidak diperlukan) untuk mengurangi titik masuk bagi peretas.

Konfigurasi IDS/IPS:

- IDS (*Intrusion Detection System*) digunakan untuk mendeteksi aktivitas mencurigakan dalam jaringan, seperti upaya masuk yang gagal berulang kali atau paket data aneh.
- IPS (*Intrusion Prevention System*) bertindak lebih lanjut dengan memblokir serangan sebelum

mencapai perangkat IoT, misalnya mencegah serangan DDoS atau *brute force login*.

- Pastikan IDS/IPS diperbarui dengan database ancaman terbaru agar dapat mengenali pola serangan terbaru.

2. Mengaktifkan Enkripsi dan Autentikasi Jaringan

Keamanan komunikasi sangat penting dalam jaringan IoT, sehingga diperlukan enkripsi serta autentikasi yang kuat untuk melindungi data dari penyadapan atau manipulasi.

Konfigurasi Enkripsi:

- Gunakan WPA3 untuk Wi-Fi: Hindari WEP atau WPA2 yang rentan terhadap serangan *brute force* (Kohlhos & Hayajneh, 2018).
- Aktifkan VPN (*Virtual Private Network*) jika *router* atau *gateway* mendukungnya, untuk mengenkripsi lalu lintas jaringan yang keluar masuk ke internet.
- Gunakan TLS (*Transport Layer Security*) atau SSL (*Secure Sockets Layer*) dalam komunikasi antar perangkat IoT dan *cloud* untuk memastikan data tetap aman.

Konfigurasi Autentikasi:

- Nonaktifkan SSID *broadcasting* agar jaringan tidak terlihat oleh perangkat yang tidak dikenal.
- Gunakan autentikasi berbasis sertifikat untuk perangkat IoT yang terhubung ke *gateway*.
- Batasi akses administrator hanya untuk perangkat atau pengguna tertentu, dan gunakan autentikasi dua faktor (2FA) untuk login ke *router/gateway*.

7.7.3 Implementasi *Firewall* dan IDS/IPS pada Jaringan IoT

Keamanan jaringan dalam IoT sangat penting untuk melindungi perangkat dari berbagai ancaman siber. Salah satu metode utama dalam mengamankan jaringan IoT adalah dengan menerapkan *Firewall* dan *Intrusion Detection*

System (IDS) serta *Intrusion Prevention System* (IPS). Implementasi sistem ini bertujuan untuk mencegah akses tidak sah, mendeteksi aktivitas mencurigakan, serta memblokir serangan sebelum mencapai perangkat IoT.

1. Implementasi *Firewall* dalam Jaringan IoT

Firewall berfungsi sebagai penghalang antara jaringan IoT dan jaringan eksternal, seperti internet. *Firewall* membantu menyaring lalu lintas data berdasarkan aturan keamanan yang telah ditetapkan untuk mencegah akses tidak sah atau serangan berbahaya. Berikut ini langkah Implementasi *Firewall* pada Jaringan IoT:

- 1) Mengonfigurasi Aturan Akses (*Access Control Lists - ACLs*)
 - Hanya mengizinkan perangkat dan layanan tertentu untuk berkomunikasi melalui jaringan.
 - Memblokir akses dari alamat IP yang mencurigakan atau berasal dari wilayah yang tidak relevan.
- 2) Menutup *Port* yang Tidak Diperlukan
Banyak serangan terjadi karena port yang tidak digunakan tetap terbuka. Oleh karena itu, hanya port yang diperlukan untuk komunikasi IoT yang harus dibiarkan aktif.
- 3) Menggunakan *Firewall* Berbasis Perangkat dan Jaringan
 - *Firewall* Perangkat (*Host-Based Firewall*): Diterapkan langsung pada perangkat IoT untuk menyaring lalu lintas masuk dan keluar.
 - *Firewall* Jaringan (*Network-Based Firewall*): Dipasang di *gateway* atau *router* untuk mengontrol lalu lintas seluruh jaringan IoT.

- 4) Menerapkan *Deep Packet Inspection* (DPI)
DPI memungkinkan firewall untuk memeriksa isi paket data guna mendeteksi pola yang mencurigakan atau serangan yang terselubung dalam lalu lintas yang tampak normal.
2. Implementasi IDS/IPS dalam Jaringan IoT
Selain *firewall*, *Intrusion Detection System* (IDS) dan *Intrusion Prevention System* (IPS) berfungsi untuk mendeteksi dan mencegah serangan siber pada jaringan IoT. Perbedaan IDS dan IPS disajikan pada tabel (Ashoor & Gore, 2011).

Tabel 7. 4 Perbedaan IDS dan IPS

Aspek	<i>Intrusion Detection System</i> (IDS)	<i>Intrusion Prevention System</i> (IPS)
Fungsi Utama	Mendeteksi dan memberikan peringatan jika ada aktivitas mencurigakan dalam jaringan	Mendeteksi dan secara otomatis mencegah serta memblokir ancaman yang terdeteksi
Respon terhadap Ancaman	Hanya memantau dan melaporkan aktivitas mencurigakan tanpa mengambil tindakan langsung.	Dapat memblokir atau menghentikan ancaman secara otomatis sebelum mencapai target.
Posisi dalam Jaringan	Biasanya ditempatkan sebagai sensor pasif yang hanya memantau lalu lintas jaringan.	Berfungsi sebagai penghalang aktif di jalur lalu lintas jaringan, sehingga dapat menyaring dan memblokir ancaman.
Dampak pada	Tidak	Dapat menyebabkan

Aspek	<i>Intrusion Detection System (IDS)</i>	<i>Intrusion Prevention System (IPS)</i>
Kinerja Jaringan	mempengaruhi lalu lintas jaringan karena hanya menganalisis data tanpa mengubahnya.	sedikit latensi karena harus memeriksa dan memproses lalu lintas sebelum meneruskannya.
Cara Kerja	Menggunakan database tanda tangan serangan atau analisis perilaku untuk mendeteksi ancaman.	Menggunakan metode serupa dengan IDS, tetapi dengan tambahan mekanisme untuk mengambil tindakan pencegahan secara real-time.
Kelebihan	- Tidak mengganggu aliran data dalam jaringan. - Dapat memberikan laporan dan analisis mendetail mengenai serangan.	- Mampu menghentikan serangan sebelum merusak sistem. - Memberikan perlindungan aktif terhadap ancaman siber.
Kekurangan	- Tidak dapat mencegah serangan, hanya memberi peringatan. - Memerlukan tindakan manual untuk menangani ancaman.	- Dapat menyebabkan false positive yang berpotensi memblokir lalu lintas jaringan yang sah. - Membutuhkan lebih banyak sumber daya dan konfigurasi yang kompleks.
Contoh Alat	Snort (Mode IDS), Suricata, Zeek (Bro IDS)	Snort (Mode IPS), Palo Alto, Cisco Firepower, Suricata (Mode IPS)

IDS lebih berfokus pada deteksi dan pelaporan, sedangkan IPS bertindak lebih lanjut dengan mencegah serangan secara otomatis. Kombinasi keduanya sangat disarankan untuk perlindungan jaringan yang lebih optimal.

Beberapa Langkah Implementasi IDS/IPS pada Jaringan IoT diantaranya:

1. Menempatkan IDS/IPS pada Titik Strategis
IDS/IPS dapat dipasang di *gateway* IoT atau pada perangkat *edge computing* untuk memantau lalu lintas data antara perangkat IoT dan jaringan eksternal.
2. Menggunakan Sistem Berbasis AI dan *Machine Learning*
Teknologi ini membantu IDS/IPS dalam mengenali pola serangan baru secara otomatis, sehingga tidak hanya mengandalkan aturan statis.
3. Mengintegrasikan IDS/IPS dengan SIEM (*Security Information and Event Management*)
SIEM memungkinkan analisis data keamanan secara real-time dan membantu administrator dalam mengambil keputusan cepat terkait ancaman.
4. Memperbarui Database Ancaman Secara Berkala
IDS/IPS harus selalu diperbarui agar dapat mengenali jenis serangan terbaru, seperti DDoS berbasis IoT, serangan *malware*, atau eksploitasi protokol komunikasi.

7.7.4 Simulasi *Penetration Testing* pada IoT

Penetration Testing pada perangkat IoT adalah proses pengujian keamanan yang bertujuan untuk mengidentifikasi kerentanan dalam sistem dan jaringan IoT sebelum dimanfaatkan oleh peretas. Dengan melakukan simulasi serangan, organisasi dapat memahami kelemahan dalam infrastruktur mereka dan menerapkan langkah-langkah mitigasi yang tepat.

1. Tahapan Simulasi Penetration Testing pada IoT

1) Perencanaan dan Pengumpulan Informasi

Pada tahap ini, tim penguji melakukan identifikasi perangkat IoT yang akan diuji, termasuk jenis perangkat keras, sistem operasi, protokol komunikasi, dan layanan yang berjalan. Informasi ini dikumpulkan melalui teknik seperti:

- *Passive Reconnaissance* (pengamatan tanpa interaksi langsung, seperti pencarian data di internet).
- *Active Reconnaissance* (menggunakan alat seperti Nmap untuk memetakan perangkat dalam jaringan).

2) Pemindaian dan Analisis Kerentanan

Tim penguji melakukan pemindaian keamanan untuk menemukan kelemahan dalam perangkat IoT menggunakan alat seperti:

- Nmap untuk memeriksa port terbuka dan layanan yang berjalan.
- Shodan untuk mencari perangkat IoT yang terhubung ke internet dan rentan terhadap eksploitasi.
- OpenVAS atau Nessus untuk mengidentifikasi kelemahan yang diketahui dalam firmware atau sistem perangkat.

3) Eksploitasi dan Pengujian Serangan

Setelah menemukan celah keamanan, tim penguji mencoba mengeksploitasinya dengan teknik seperti:

- Serangan DDoS: Mensimulasikan serangan dengan membanjiri perangkat IoT menggunakan alat seperti LOIC atau Hping3.
- *Man-in-the-Middle Attack* (MITM): Mencegat komunikasi antara perangkat dengan menggunakan Ettercap atau Wireshark.

- *Eksplorasi Firmware*: Menganalisis *firmware* perangkat untuk menemukan kerentanan menggunakan *Binwalk* atau *Firmware Mod Kit*.

4) Evaluasi Hasil dan Dokumentasi

Evaluasi hasil bertujuan untuk menilai efektivitas dan efisiensi sistem IoT yang telah dikembangkan.

Proses evaluasi mencakup:

- Pengukuran Kinerja: Menggunakan metrik seperti latensi, *throughput*, akurasi sensor, konsumsi daya, dan keandalan jaringan.
- Analisis Data: Memeriksa data yang dikumpulkan dari sensor untuk memastikan bahwa informasi yang dihasilkan akurat dan sesuai dengan kebutuhan pengguna.
- Uji Keandalan: Menguji sistem dalam berbagai kondisi lingkungan untuk memastikan bahwa perangkat IoT dapat beroperasi secara stabil.
- Keamanan dan Privasi: Mengevaluasi apakah sistem memiliki perlindungan terhadap ancaman keamanan seperti serangan siber dan kebocoran data.
- *User Experience (UX)*: Jika IoT digunakan oleh pengguna akhir, penting untuk mengukur sejauh mana kemudahan penggunaan dan manfaat yang diperoleh.

Dokumentasi dalam proyek IoT sangat krusial untuk pemeliharaan, pengembangan lebih lanjut, serta referensi di masa depan. Dokumentasi mencakup:

- Dokumentasi Teknis: Berisi spesifikasi perangkat keras, perangkat lunak, arsitektur

sistem, protokol komunikasi, dan konfigurasi jaringan.

- Log Data dan Analisis: Mencatat data historis dan hasil analisis yang dapat digunakan untuk perbaikan dan pengembangan lebih lanjut.
- Manual Pengguna: Jika perangkat IoT digunakan oleh pengguna lain, maka panduan penggunaan, instalasi, dan pemecahan masalah perlu disediakan.
- Laporan Evaluasi: Dokumen yang mencakup hasil pengujian, temuan masalah, dan rekomendasi perbaikan atau pengembangan lebih lanjut.

Tahap evaluasi dan dokumentasi membantu memastikan bahwa sistem IoT tidak hanya berfungsi optimal tetapi juga dapat dikembangkan dan diperbaiki dengan lebih mudah di masa depan

5) Perbaikan dan Pengujian Ulang

Setelah implementasi langkah-langkah perbaikan, pengujian ulang dilakukan untuk memastikan bahwa celah keamanan telah tertutup.

2. Alat yang Digunakan dalam Simulasi *Penetration Testing IoT*

Berikut adalah tabel yang berisi alat-alat yang digunakan dalam simulasi *Penetration Testing IoT* disajikan pada tabel berikut ini:

Tabel 7. 5 Alat yang Digunakan dalam Simulasi *Penetration Testing IoT*

Kategori	Nama Alat	Fungsi
<i>Sniffing Monitoring</i> &	<i>Wireshark</i>	Menganalisis lalu lintas jaringan untuk mendeteksi kelemahan komunikasi.
	<i>Tcpdump</i>	Alat berbasis command-line untuk menangkap dan

Kategori	Nama Alat	Fungsi
		menganalisis paket jaringan.
<i>Scanning & Enumeration</i>	<i>Nmap</i>	Memindai jaringan untuk menemukan perangkat IoT yang terhubung dan layanan yang berjalan.
	<i>Angry IP Scanner</i>	Memindai jaringan untuk mengidentifikasi perangkat yang aktif.
<i>Exploitation</i>	<i>Metasploit Framework</i>	Framework untuk mengeksploitasi kerentanan sistem IoT dan menguji keamanannya.
	<i>RouterSploit</i>	Alat eksploitasi khusus untuk perangkat IoT, seperti router dan kamera IP.
<i>Firmware Analysis</i>	<i>Binwalk</i>	Menganalisis dan mengekstrak isi firmware dari perangkat IoT.
	<i>Firmadyne</i>	Alat untuk melakukan emulasi dan analisis firmware.
<i>Reverse Engineering</i>	<i>IDA Pro</i>	Digunakan untuk membongkar kode biner firmware perangkat IoT.
	<i>Ghidra</i>	Alat reverse engineering open-source untuk menganalisis perangkat lunak tertanam dalam IoT.
<i>Radio Frequency (RF) Testing</i>	<i>HackRF One</i>	Digunakan untuk menguji keamanan komunikasi berbasis RF pada perangkat IoT.
	<i>RTL-SDR</i>	Alat untuk mendeteksi dan menganalisis sinyal nirkabel yang digunakan oleh perangkat IoT.

Kategori	Nama Alat	Fungsi
<i>Web & API Security Testing</i>	<i>Burp Suite</i>	Menganalisis dan menguji keamanan API serta komunikasi web perangkat IoT.
	<i>Postman</i>	Menguji endpoint API dari perangkat IoT untuk melihat potensi kelemahan.
<i>Brute Force & Credential Attacks</i>	<i>Hydra</i>	Alat untuk mencoba serangan brute force pada kredensial perangkat IoT.
	<i>John the Ripper</i>	Digunakan untuk memecahkan password yang digunakan dalam perangkat IoT.

Alat-alat ini membantu mengidentifikasi, mengeksploitasi, dan memperbaiki celah keamanan dalam sistem IoT sebelum serangan terjadi. Penting untuk menemukan serta mengatasi kerentanan sebelum diserang. Dengan perencanaan, pemindaian, eksploitasi, dan evaluasi, organisasi dapat memastikan perangkat IoT mereka memiliki pertahanan yang kuat terhadap ancaman siber.

DAFTAR PUSTAKA

- Aas, J., Durumeric, Z., Alex Halderman, J., Rescorla, E., Barnes, R., Eckersley, P., Hoffman-Andrews, J., Schoen, S., Case, B., Flores-López, A., Kasten, J., & Warren, B. (2019). Let's encrypt: An automated certificate authority to encrypt the entire web. *Proceedings of the ACM Conference on Computer and Communications Security*, 2473–2487. <https://doi.org/10.1145/3319535.3363192>
- Agustina, A. N., Aryanti, & Nasron. (2017). Pengamanan Dokumen Menggunakan Metode Rsa (Rivest Shamir Adleman) Berbasis Web. *Proceeding SENDI_U*, 3(3), 14–19.
- Andriani, Y. F., Noor, M. F., Salim, A. S., & Hanafi. (2019). Internet Of Things (Iot) – Tantangan Dan Keamanan Iot Menggunakan Enkripsi AES. *Jurnal INFORMA Politeknik Indonusa Surakarta*, 5(1), 76–83. [http://download.garuda.ristekdikti.go.id/article.php?article=1706002&val=18526&title=INTERNET OF THINGS IOT TANTANGAN DAN KEAMANAN IOT MENGGUNAKAN ENKRIPSI AES](http://download.garuda.ristekdikti.go.id/article.php?article=1706002&val=18526&title=INTERNET%20OF%20THINGS%20IOT%20TANTANGAN%20DAN%20KEAMANAN%20IOT%20MENGUNAKAN%20ENKRIPSI%20AES)
- Ashoor, A. S., & Gore, S. (2011). Difference between Intrusion Detection System (IDS) and Intrusion Prevention System (IPS). *Communications in Computer and Information Science*, 196 CCIS, 497–501. https://doi.org/10.1007/978-3-642-22540-6_48
- Culot, G., Nassimbeni, G., Podrecca, M., & Sartor, M. (2021). The ISO/IEC 27001 information security management standard: literature review and theory-based research agenda. *TQM Journal*, 33(7), 76–105. <https://doi.org/10.1108/TQM-09-2020-0202>
- Dotsenko, S., Illiashenko, O., Kamenskyi, S., & Kharchenko, V. (2019). Integrated Model of Knowledge Management for Security of Information Technologies: Standards ISO/IEC 15408 and ISO/IEC 18045. *Information & Security: An International Journal*, 43(3), 305–317. <https://doi.org/10.11610/isij.4323>

- Erlangung, Z., & Master, G. (2023). *Masterarbeit*.
- Ferraiolo, D. F., Cugini, J. A., & Kuhn, D. R. (1995). RBAC-Features and Motivations. In *11th Annual Computer Security Applications Proceedings*. <http://csrc.nist.gov/groups/SNS/rbac/documents/ferraiolo-cugini-kuhn-95.pdf>
- Guston, D. (2012). National Institute of Standards and Technology (U.S.). *Encyclopedia of Nanoscience and Society*. <https://doi.org/10.4135/9781412972093.n332>
- Hu, V. C., Ferraiolo, D., Kuhn, R., Schnitzer, A., Sandlin, K., Miller, R., & Scarfone, K. (2014). Guide to attribute based access control (abac) definition and considerations. *NIST Special Publication, 800*, 162.
- Khamsyar, A., & Basri, M. (2022). Aplikasi Enkripsi Gambar Menggunakan Metode (Rivest Shamir Adleman) Rsa. *Jurnal Sintaks Logika*, 2(3), 39–45. <https://doi.org/10.31850/jsilog.v2i3.1850>
- Kohlhos, C. P., & Hayajneh, T. (2018). A comprehensive attack flow model and security analysis for Wi-Fi and WPA3. *Electronics (Switzerland)*, 7(11). <https://doi.org/10.3390/electronics7110284>
- Marikyan, D., Papagiannidis, S., Ranjan, R., & Rana, O. (2021). General data protection regulation: An individual's perspective. *ACM International Conference Proceeding Series, May*. <https://doi.org/10.1145/3492323.3495620>
- Mauliddiyah, N. L. (2021). ANALISIS PENDETEKSIAN SERANGAN DENIAL OF SERVICE (DOS) MENGGUNAKAN LOGIKA FUZZY METODE MAMDANI PADA JARINGAN INTERNET OF THINGS (IOT). 8(1), 6.
- Polemi, N. (n.d.). *CYBER SECURITY A Proposed Cyber Security Certification Scheme for Supply Chain Services*. 50–56.
- Putra, Y., Yuhandri, Y., & Sumijan, S. (2021). Meningkatkan Keamanan Web Menggunakan Algoritma Advanced Encryption Standard (AES) terhadap Serangan Cross Site Scripting. *Jurnal Sistim Informasi Dan Teknologi*. <https://doi.org/10.37034/jsisfotek.v3i2.44>
- Rafsanjani, M. S., Suryani, V., & Pahlevi, R. R. (2022). Deteksi Serangan Botnet Pada Jaringan Internet of Things

- Menggunakan Algoritma Random Forest (RF). *E-Proceeding of Engineering*, 9(3), 1862–1871.
- Saputro, T. H., Hidayati, N. H., & H. Ujianto, E. I. (2020). Survei Tentang Algoritma Kriptografi Asimetris. *Jurnal Informatika Polinema*, 6(2), 67–72. <https://doi.org/10.33795/jip.v6i2.345>
- Sari, R., Zain, A. R., & Cakraningrat, M. S. (2023). Implementasi Enkripsi Dekripsi Paket Data pada Rancang Bangun Smart Home Menggunakan Protokol MQTT. *Multinetics*, 8(2), 168–176. <https://doi.org/10.32722/multinetics.v8i2.4110>
- Sutanto, F., Yulianton, H., & Razaq, J. (2011). Rancang Bangun VLAN untuk Segmentasi Jaringan pada Cyber Campus Laboratory Universitas Stikubank. *None*, 16(2), 245934.
- Syahputri, N. I., Harahap, H., Siregar, R., & Tommy, T. (2023). Penyuluhan Pentingnya Two Factor Authentication dan Aplikasinya Di Era Keamanan Digital. *Jurnal Pengabdian Masyarakat Bangsa*, 1(6), 768–773. <https://doi.org/10.59837/jpmba.v1i6.256>

BAB 8

IMPLEMENTASI IoT PADA INDUSTRI MANUFAKTUR

Oleh Frabowo Prasetia

8.1 Implementasi IoT pada Industri

Internet of Things (IoT) telah mengubah lanskap industri secara signifikan dalam beberapa tahun terakhir. Dengan memanfaatkan konektivitas internet dan sensor-sensor yang terhubung, perusahaan dapat mengoptimalkan proses produksi, meningkatkan efisiensi operasional, dan memberikan layanan yang lebih baik kepada pelanggan. Dalam materi ini, kita akan mengeksplorasi beberapa contoh implementasi IoT yang sukses dalam industri (Lee, et al., 2015).

1. *Monitoring* dan Pemeliharaan Peralatan

Salah satu penerapan utama IoT dalam industri adalah monitoring dan pemeliharaan peralatan. Dengan menginstal sensor pada mesin dan peralatan pabrik, perusahaan dapat secara real-time memantau kondisi mereka. Data yang dikumpulkan oleh sensor ini dapat memberikan wawasan yang berharga tentang kesehatan peralatan, memungkinkan perawatan preventif yang lebih efisien untuk mencegah kerusakan dan *downtime* yang tidak terduga (Lee, et al., 2015).

Contoh: Perusahaan manufaktur otomotif menggunakan sensor IoT pada mesin produksi mereka untuk memantau suhu, tekanan, dan getaran. Dengan menganalisis data sensor secara *real-time*, mereka dapat mendeteksi potensi kegagalan peralatan dan melakukan perawatan sebelum terjadi kerusakan serius.

2. *Supply Chain Management*

IoT juga telah mengubah cara perusahaan mengelola rantai pasokan mereka. Dengan memasang sensor pada produk dan kemasannya, perusahaan dapat melacak lokasi dan kondisi barang secara *real-time* selama transit. Hal ini memungkinkan visibilitas yang lebih baik dalam rantai pasokan, memungkinkan perencanaan yang lebih baik, pengelolaan persediaan yang lebih efisien, dan pengiriman yang tepat waktu (Lee, et al., 2015).

Contoh: Perusahaan logistik menggunakan sensor IoT pada kemasan barang untuk melacak posisi dan kondisi mereka selama pengiriman. Dengan memantau suhu dan kelembaban, mereka dapat memastikan bahwa produk yang sensitif terhadap lingkungan tetap dalam kondisi optimal selama transit (Lee, et al., 2015).

3. Pengoptimalan Proses Produksi

Dengan menghubungkan peralatan produksi ke jaringan IoT, perusahaan dapat meningkatkan efisiensi dan produktivitas proses manufaktur mereka. Data yang dikumpulkan oleh sensor dapat digunakan untuk mengidentifikasi *bottleneck*, mengoptimalkan aliran kerja, dan mengurangi pemborosan. Ini memungkinkan perusahaan untuk menghasilkan lebih banyak produk dengan biaya yang lebih rendah (Lee, et al., 2015).

Contoh: Pabrik farmasi menggunakan sensor IoT pada mesin pengemasan mereka untuk memantau kecepatan dan efisiensi produksi. Dengan menganalisis data sensor, mereka dapat mengidentifikasi area di mana produktivitas dapat ditingkatkan dan mengimplementasikan perubahan yang diperlukan.

4. Pelayanan Pelanggan Berbasis IoT

IoT juga memungkinkan perusahaan untuk memberikan layanan yang lebih baik kepada pelanggan mereka. Dengan menghubungkan produk ke internet, perusahaan dapat mengumpulkan data tentang penggunaan dan performa produk secara *real-time*. Ini memungkinkan perusahaan untuk menawarkan layanan pelanggan yang

lebih personal dan proaktif, seperti pemeliharaan terjadwal atau upgrade produk (Lee, et al., 2015).

Contoh: Produsen peralatan rumah tangga cerdas menggunakan sensor IoT pada produk mereka untuk mengumpulkan data tentang penggunaan dan kinerja. Dengan menganalisis data ini, mereka dapat memberikan rekomendasi kepada pelanggan tentang cara meningkatkan efisiensi energi atau melakukan perawatan preventif.

8.2 Siklus Manufaktur: Langkah-langkah dalam Proses Produksi

Konsumen

Istilah yang sering digunakan oleh beberapa customer yakni (Groover, 2012):

1. *Client*

Client atau dalam Bahasa Indonesia klien adalah seseorang atau sekelompok organisasi yang ahli di bidangnya (professional).

2. *Costumer*

Costumer atau pelanggan adalah seorang yang membeli suatu barang namun barang tersebut tidak digunakan atau dikonsumsi. Biasanya seorang *costumer* akan memberikan barang yang belinya tersebut kepada seorang *consumer* atau konsumen sebagai *end user*.

3. *Consumer*

Terdapat tiga pengertian dari konsumen atau *consumer* yakni:

- a. Pengguna barang (pakaian, bahan, makanan, minuman, dan sebagainya)
- b. Pengguna jasa
- c. Pemakai jasa

Pengertian diatas menjelaskan bahwa seorang konsumen bukan hanya sebagai pembeli barang tetapi juga sebagai pengguna atau seseorang yang mengonsumsi barang yang dibelinya. Namun, seseorang yang membeli barang kemudian dikonsumsi untuk dirinya sendiri, hal tersebut

dikatakan sebagai seorang *costumer* bukan sebagai *consumer* atau konsumen.

Perancangan Produk

Salah satu kunci agar suatu perusahaan mengalami perkembangan yang baik adalah dengan melakukan pengembangan suatu produk dan perbaikan secara *real-time* agar produk tersebut tidak kehilangan pasar (Groover, 2012).

Hal-hal yang perlu dilakukan dalam melakukan proses perancangan produk yakni:

- a. Pengembangan ide-ide seperti hal nya pada bidang teknologi dan pangsa pasar.
- b. Melakukan identifikasi masukan ide yang baik untuk perusahaan. Namun dalam penentuan ide tersebut dilakukan beberapa analisis pengujian seperti:
 1. Potensi pasar
 2. Pemasukan yang diterima
 3. Kesesuaian produk
 4. Produk yang dihasilkan harus memiliki spesifikasi design yang menarik seperti teknologi, kualitas, tampilan produk, dan lain-lain.
- c. Melakukan perancangan dengan menggunakan prototipe. Hal ini dilakukan untuk melihat dalam bentuk design yang menyerupai produk tersebut sebelum diproduksi.
- d. Membuat beberapa produk prototipenya
- e. Hasil prototipe yang dibuat akan dilakukan pengujian dengan data kuantitatif (survey pelanggan terkait produk yang akan diproduksi), design kemasan produk, revisi hasil dari pengujian yang dilakukan.
- f. Melakukan produksi barang, perancangan, dan penginstalan
- g. Melakukan uji kembali hasil produk awal yang telah dilakukan untuk menentukan produk tersebut siap diproduksi massal.
- h. Proses produksi produk.

Adapun kendala-kendala yang sering terjadi pada perancangan produk yakni (Groover, 2012):

- a. Kurangnya ide-ide yang menyesuaikan dengan perkembangan yang ada
- b. Adanya persaingan antar perusahaan lain yang begitu ketat sehingga perlu dalam menghasilkan produk yang berkualitas dan harga jual tinggi
- c. Produk yang dihasilkan harus bersertifikasi atau berlabel aman dalam hal ini telah bersertifikat BPOM
- d. Biaya yang diperlukan dalam produksi produk baru biasanya membutuhkan biaya yang begitu besar.

Perancangan Proses

Perlu pemahaman yang mendasar terkait dengan sistem produktif yakni produk yang memiliki kuantitas baik. Pentingnya keputusan ini diambil oleh seorang pimpinan manajer untuk menentukan proses dari produksi berupa barang dan jasa (Kalpakjian, 1995).

Perancangan Produksi

Suatu langkah dalam menciptakan suatu produk dan mengikut langkah-langkah sehingga produk dapat bias di pasarkan. Perusahaan juga sebaiknya perlu *plan* atau strategi lain sebagai langkah jika terjadi produk gagal dalam pemasaran. Metode perancangan yakni penyesuaian suatu masalah yang terjadi agar perancangan tersebut dapat menghasilkan suatu produk. Dengan adanya metode perancangan produk akan memudahkan dalam proses perancangan (Kalpakjian, 1995).

Proses Produksi

Proses produksi yakni penggabungan antara factor produksi yang ada untuk menciptakan suatu produk yang menghasilkan manfaat bagi konsumen. Adapun tujuan dari suatu proses produksi antara lain (Kalpakjian, 1995):

1. Menghasilkan produk berupa barang dan jasa
2. Menjaga perekonomian suatu perusahaan
3. Adanya nilai yang diberikan terhadap produk

4. Mendapat keuntungan dengan pencapaian agar tercapainya kemakmuran
5. Dapat mengganti produk yang telah rusak, kadaluarsa (*expired*)
6. Memenuhi permintaan pasar baik dari domestik maupun international agar dapat bersaing ke luar negeri.

Karakteristik atau Ciri-Ciri Proses Produksi

Beberapa ciri-ciri dari proses produksi berdasarkan proses, sifat dan jangka waktu sebagai berikut (Groover, 2012):

1. Berdasarkan proses
 - a. Proses Langsung yakni suatu kegiatan meliputi produksi primer dan sekunder. Produksi primer adalah suatu kegiatan dimana proses ini terjadi pada alam secara langsung seperti contoh pada pertambangan, perikanan, pertanian, dan lain-lain. Produksi sekunder adalah proses produksi ini menambah nilai pada barang atau jasa seperti contoh kayu untuk membuat meja atau kursi, baja sebagai bahan untuk membuat jembatan.
 - b. Produksi tidak langsung yakni kegiatan suatu produksi kemudian memberikan nilai tambahan pada keahlian atau jasanya seperti contoh jasa kesehatan, jasa montir, jasa konsultasi.
2. Berdasarkan Sifat Proses Produksi

Terdapat beberapa sifat yang perlu diketahui dalam proses suatu produksi sebagai berikut:

 - a. Proses ekstraktif yakni produksi langsung dari alam dalam menghasilkan produk
 - b. Proses analitik yakni proses produksi yang memisahkan suatu produk menjadi produk yang menyerupai asli dan diproduksi dalam jumlah banyak.
 - c. Proses fabrikasi yakni proses perubahan bahan baku menjadi produk yang berguna.
 - d. Proses sintetik yakni penggabungan beberapa bahan sehingga menghasilkan produk yang disesuaikan dalam hal ini dimaksudkan adalah proses perakitan.

3. Berdasarkan Jangka Waktu

- a. Proses secara *Real-Time* yakni proses produksi yang dilakukan secara terus menerus tanpa mengenal waktu. Biasanya proses produksi ini dilakukan dalam skala besar atau jumlah besar.
- b. Produksi secara terputus-putus yakni proses produksi yang dilakukan ketika terdapat pesanan saja, ketika perusahaan memiliki pesanan maka akan baru dikerjakan proses produknya.

Pengendalian Persediaan

Pengendalian persediaan dilakukan dengan cara melihat kondisi stok produk sehingga dalam proses persediaan barang tidak terjadi *over stock*. Jika terjadi *over stock* pada suatu perusahaan akan mengakibatkan terjadinya pembengkakan pada biaya sehingga kegiatan tersebut adalah suatu hal pemborosan (Groover, 2012).

Pengendalian Kualitas

Kualitas ini biasanya menjadi penilaian pada seorang konsumen, “ada harga ada kualitas”. Semakin tinggi harga yang diberikan kualitas suatu barang juga akan mejadi lebih baik. Namun, pada bidang manufakturm kualitas dapat diartikan sebagai kinerja yang lebih baik, fitur yang lebih baik serta *maintenance* adalah bagian yang membutuhkan biaya yang begitu besar pula (Kalpakjian, 1995).

Teknik suatu pengendalian kualitas adalah teknik yang bermanfaat dikarenakan suatu perusahaan produksi biasanya sebelum melakukan pemasaran produk dilakukan terlebih dahulu uji kualitas produk apakah layak dipasarkan atau belum (Kalpakjian, 1995).

Pengendalian Produksi

Pada bagian ini dilakukan langkah/prosedur yang mengarahkan semua dalam proses produksi yakni proses produksi, standar kualitas produksi, sumber daya manusia sehingga proses produksi dapat diperoleh dengan biaya rendah dan waktu yang cepat. Fungsi pengendalian produksi pada

perusahaan antara lain perencanaan, penentuan urutan kerja, penentuan waktu kerja, pemberian perintah, tindak lanjut (Groover, 2012).

Supplier

Biasanya supplier ini adalah pihak yang melakukan penjualan atau penyedia bahan siap olah dan akan diberikan kepada pihak atau mitra lain. Adapun ciri-ciri dari *supplier* yakni: sebagai pemasok bahan baku, produk yang dijual berbentuk bahan mentah siap olah (Groover, 2012).

8.3 Implementasi *Internet of Things* (IoT) dalam Pengelolaan Proses

Internet of Things (IoT) telah merevolusi cara perusahaan mengelola proses mereka. Dengan menghubungkan perangkat dan sensor ke internet, perusahaan dapat memantau, mengontrol, dan mengoptimalkan proses secara real-time. Dalam materi ini, kita akan menjelajahi bagaimana IoT digunakan dalam pengelolaan proses untuk meningkatkan efisiensi, keandalan, dan produktivitas (Lee, et al., 2015).

1. Pemantauan dan Pengumpulan Data

Penerapan utama IoT dalam pengelolaan proses adalah kemampuannya untuk memantau dan mengumpulkan data secara *real-time*. Dengan memasang sensor pada peralatan dan infrastruktur, perusahaan dapat mengumpulkan informasi tentang suhu, kelembaban, tekanan, dan parameter lainnya yang penting untuk proses produksi (Lee, et al., 2015).

Contoh: Pabrik kimia menggunakan sensor IoT pada tangki penyimpanan untuk memantau tingkat dan suhu zat kimia. Data yang dikumpulkan ini membantu mereka dalam memantau kondisi penyimpanan dan mencegah kebocoran atau kebocoran yang tidak diinginkan.

2. Analisis Data dan Prediksi

Data yang dikumpulkan oleh sensor IoT dapat dianalisis menggunakan teknik kecerdasan buatan (AI) dan

analitik data untuk mendapatkan wawasan yang berharga tentang kinerja proses. Dengan memahami pola dan tren dalam data, perusahaan dapat membuat prediksi tentang potensi kegagalan atau perbaikan yang diperlukan (Lee, et al., 2015).

Contoh: Pabrik otomotif menggunakan analisis data IoT untuk memprediksi waktu pemeliharaan mesin. Dengan memantau kinerja mesin secara *real-time*, mereka dapat mengidentifikasi potensi kerusakan dan menjadwalkan perawatan preventif sebelum terjadi gangguan produksi .

3. Otomatisasi dan Kontrol Proses

IoT memungkinkan otomatisasi yang lebih lanjut dalam pengelolaan proses. Dengan menghubungkan perangkat ke internet, perusahaan dapat mengontrol operasi proses secara otomatis berdasarkan data yang diterima dari sensor. Hal ini memungkinkan untuk reaksi cepat terhadap perubahan kondisi dan pengoptimalan secara real-time (Lee, et al., 2015).

Contoh: Pabrik makanan menggunakan sistem otomatisasi IoT untuk mengontrol suhu dan waktu proses pada oven pemanggangan. Sistem ini dapat menyesuaikan suhu dan waktu secara otomatis berdasarkan jenis dan jumlah produk yang dimasukkan, memastikan konsistensi dan kualitas produk.

4. Pengembangan Proses Berbasis IoT

Dengan memanfaatkan IoT, perusahaan dapat mengembangkan proses baru atau meningkatkan proses yang ada untuk mencapai tingkat efisiensi yang lebih tinggi. Hal ini meliputi penggunaan teknologi seperti pemrosesan edge, komunikasi mesin ke mesin (M2M), dan integrasi dengan sistem perusahaan yang ada (Lee, et al., 2015).

Contoh: Pabrik manufaktur menggunakan teknologi IoT untuk mengembangkan sistem pemrosesan edge yang memungkinkan analisis data secara *real-time* di tempat produksi. Ini memungkinkan pengambilan keputusan yang lebih cepat dan respons yang lebih efisien terhadap perubahan kondisi.

8.4 Pemanfaatan Mesin: Meningkatkan Produktivitas dan Efisiensi Operasional

Pemanfaatan mesin adalah kunci dalam meningkatkan produktivitas dan efisiensi operasional dalam industri. Dalam era digital, penggunaan teknologi seperti Internet of Things (IoT), kecerdasan buatan (AI), dan analitik data memungkinkan perusahaan untuk memaksimalkan kinerja mesin mereka. Dalam materi ini, kita akan menjelajahi bagaimana pemanfaatan mesin dapat meningkatkan kinerja perusahaan dan menciptakan keunggulan kompetitif (Smith, et al., 2001).

1. Pemantauan Kinerja Mesin secara *Real-time*

Pemanfaatan mesin dimulai dengan pemantauan kinerja mesin secara *real-time*. Dengan memasang sensor pada mesin, perusahaan dapat memantau parameter kunci seperti suhu, tekanan, kecepatan, dan pemakaian energi. Data yang dikumpulkan ini memberikan wawasan yang berharga tentang kesehatan mesin dan memungkinkan untuk deteksi dini potensi masalah (Smith, et al., 2001).

Contoh: Pabrik manufaktur menggunakan sensor IoT pada mesin produksi mereka untuk memantau suhu dan getaran. Data yang dikumpulkan digunakan untuk menganalisis kinerja mesin dan mendeteksi potensi kegagalan sebelum terjadi.

2. Prediksi Kegagalan dan Perawatan Preventif

Dengan analisis data yang tepat, perusahaan dapat melakukan prediksi terhadap potensi kegagalan mesin dan merencanakan perawatan preventif secara efektif. Melalui penggunaan algoritma kecerdasan buatan, data historis dan real-time dapat digunakan untuk mengidentifikasi pola dan tren yang menunjukkan risiko kegagalan (Smith, et al., 2001).

Contoh: Pabrik otomotif menggunakan analitik data untuk memprediksi waktu pemeliharaan mesin. Dengan memantau kondisi mesin secara terus-menerus, mereka dapat merencanakan perawatan preventif yang sesuai dan menghindari *downtime* yang tidak terduga.

3. Optimalisasi Kinerja Mesin

Pemanfaatan mesin juga melibatkan optimalisasi kinerja mesin untuk meningkatkan produktivitas dan efisiensi. Dengan menggunakan teknologi seperti machine learning, perusahaan dapat mengoptimalkan pengaturan dan parameter operasional mesin untuk mencapai hasil terbaik (Smith, et al., 2001).

Contoh: Pabrik farmasi menggunakan machine learning untuk mengoptimalkan proses pencampuran obat. Dengan menganalisis data produksi, mereka dapat mengidentifikasi kombinasi parameter yang memberikan hasil terbaik dalam hal kualitas dan efisiensi.

4. Integrasi Sistem dan Otomatisasi

Pemanfaatan mesin juga melibatkan integrasi sistem dan otomatisasi proses. Dengan menghubungkan mesin ke sistem manajemen produksi dan mengimplementasikan kontrol otomatis, perusahaan dapat meningkatkan koordinasi antar mesin dan mengurangi keterlibatan manusia yang tidak perlu (Smith, et al., 2001).

Contoh: Pabrik elektronik menggunakan sistem SCADA (*Supervisory Control and Data Acquisition*) untuk mengontrol dan mengawasi operasi mesin secara otomatis. Ini memungkinkan mereka untuk merespons perubahan kondisi secara cepat dan menjaga konsistensi produksi.

8.5 Pemeliharaan Terprediksi: Meningkatkan Efisiensi dan Ketersediaan Mesin

Pemeliharaan terprediksi merupakan pendekatan proaktif dalam manajemen aset yang bertujuan untuk mencegah kegagalan mesin dan mengoptimalkan ketersediaan mereka. Dengan menggunakan data sensor dan analisis prediktif, perusahaan dapat merencanakan perawatan secara tepat waktu, menghindari downtime tak terduga, dan meningkatkan efisiensi operasional. Dalam materi ini, kita akan menjelajahi konsep dan manfaat dari pemeliharaan terprediksi dalam industry (Jardine, et al., 2006).

1. Konsep Pemeliharaan Terprediksi
Pemeliharaan terprediksi didasarkan pada analisis data real-time dan historis untuk mengidentifikasi pola dan tren yang menunjukkan potensi kegagalan mesin. Dengan memahami karakteristik kinerja mesin dan faktor-faktor yang mempengaruhinya, perusahaan dapat membuat model prediktif yang memungkinkan mereka untuk memprediksi waktu pemeliharaan yang optimal (Jardine, et al., 2006).
2. Pengumpulan dan Analisis Data Sensor
Pemeliharaan terprediksi membutuhkan pengumpulan data yang terus-menerus dari sensor yang terpasang pada mesin. Data ini mencakup parameter seperti suhu, tekanan, getaran, dan konsumsi energi. Melalui analisis data menggunakan teknik kecerdasan buatan, perusahaan dapat mengidentifikasi pola anomali yang menunjukkan risiko kegagalan (Jardine, et al., 2006).
3. Prediksi Kegagalan dan Perencanaan Perawatan
Berdasarkan analisis data, perusahaan dapat membuat prediksi tentang kapan mesin akan mengalami kegagalan atau memerlukan perawatan. Ini memungkinkan mereka untuk merencanakan perawatan preventif atau perbaikan secara tepat waktu, menghindari downtime tak terduga dan meminimalkan dampak negatifnya terhadap produksi (Jardine, et al., 2006).
4. Manfaat Pemeliharaan Terprediksi
 - Meningkatkan Ketersediaan Mesin: Dengan merencanakan perawatan secara tepat waktu, pemeliharaan terprediksi dapat meningkatkan ketersediaan mesin dan mengurangi downtime produksi (Jardine, et al., 2006).
 - Mengurangi Biaya Pemeliharaan: Dibandingkan dengan pemeliharaan berdasarkan jadwal atau reaktif, pemeliharaan terprediksi dapat mengurangi biaya pemeliharaan dengan mencegah kegagalan yang lebih serius dan mahal (Jardine, et al., 2006).
 - Optimalkan Sumber Daya: Dengan merencanakan perawatan berdasarkan kebutuhan aktual mesin, perusahaan dapat mengoptimalkan penggunaan

sumber daya manusia, suku cadang, dan waktu operasional (Jardine, et al., 2006).

5. Studi Kasus

Contoh: Pabrik manufaktur otomotif menggunakan pemeliharaan terprediksi untuk merawat robot pengelasan yang kritis. Melalui analisis data getaran dan suhu, mereka dapat memprediksi waktu perawatan yang optimal untuk menjaga kinerja robot dalam kondisi terbaik.

DAFTAR PUSTAKA

- Groover, M. P., 2012. *Fundamentals of Modern Manufacturing: Materials, Processes, and Systems*. USA: Jhon Wiley & Sons.
- Jardine, A. K., Lin, D. & Banjevic, D., 2006. A review on machinery diagnostics and prognostics implementing condition-based maintenance. *Mechanical Systems and Signal Processing*, 20(7), pp. 1483-1510.
- Kalpakjian, S., 1995. *Manufacturing Engineering and Technology*. New York: Addison-Wesley.
- Lee, In & Lee, J.-H., 2015. The Internet of Things (IoT): Applications, investments, and challenges for enterprises. *Business Horizons*, 58(4), pp. 431-440.
- Smith, Gary & Cooper, T., 2001. *Real-time machine utilization monitoring system and method*. United State: s.n.

BAB 9

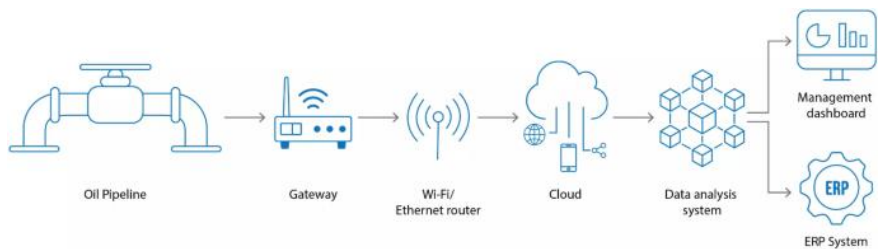
IMPLEMENTASI IOT PADA BIDANG MINYAK DAN GAS

Oleh Cahyo Wibowo



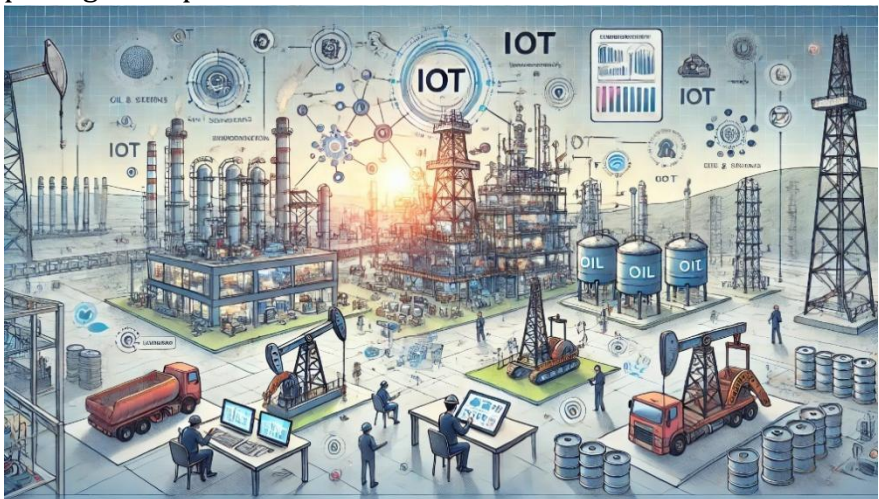
9.1 Pendahuluan

Minyak dan gas bumi (migas) yang terkandung di dalam tanah Indonesia merupakan sumber daya alam strategis yang memiliki peran penting bagi negara.[1]. Perkembangan teknologi dalam industri serta distribusi minyak dan gas menjadikan Internet of Things (IoT) sebagai bagian tak terpisahkan dari setiap aktivitas industri migas saat ini. Baik pada sektor hulu maupun hilir, penerapan IoT mencerminkan transformasi digital dalam era Industri 4.0. *Transformasi digital menjadi kebutuhan baik saat ini maupun di masa depan, sekaligus menjadi tren dalam pemanfaatan konektivitas di sektor minyak dan gas.*[2].



Gambar 9. 1 Ilustrasi Data Transfer

Pemanfaatan IoT dalam industri migas didukung oleh komputasi awan (*cloud*), kecerdasan buatan (AI), dan pembelajaran mesin (ML) untuk menyajikan informasi. Wawasan ini memungkinkan identifikasi cepat terhadap aset yang membutuhkan perhatian, mencegah kegagalan, mengurangi kebutuhan tenaga kerja, serta meminimalkan waktu henti akibat kerusakan. Selain itu, IoT meningkatkan kinerja aset, menekan risiko kecelakaan kerja dan pencemaran lingkungan, serta meningkatkan efisiensi dan produktivitas perusahaan, yang pada akhirnya berkontribusi pada peningkatan profit.



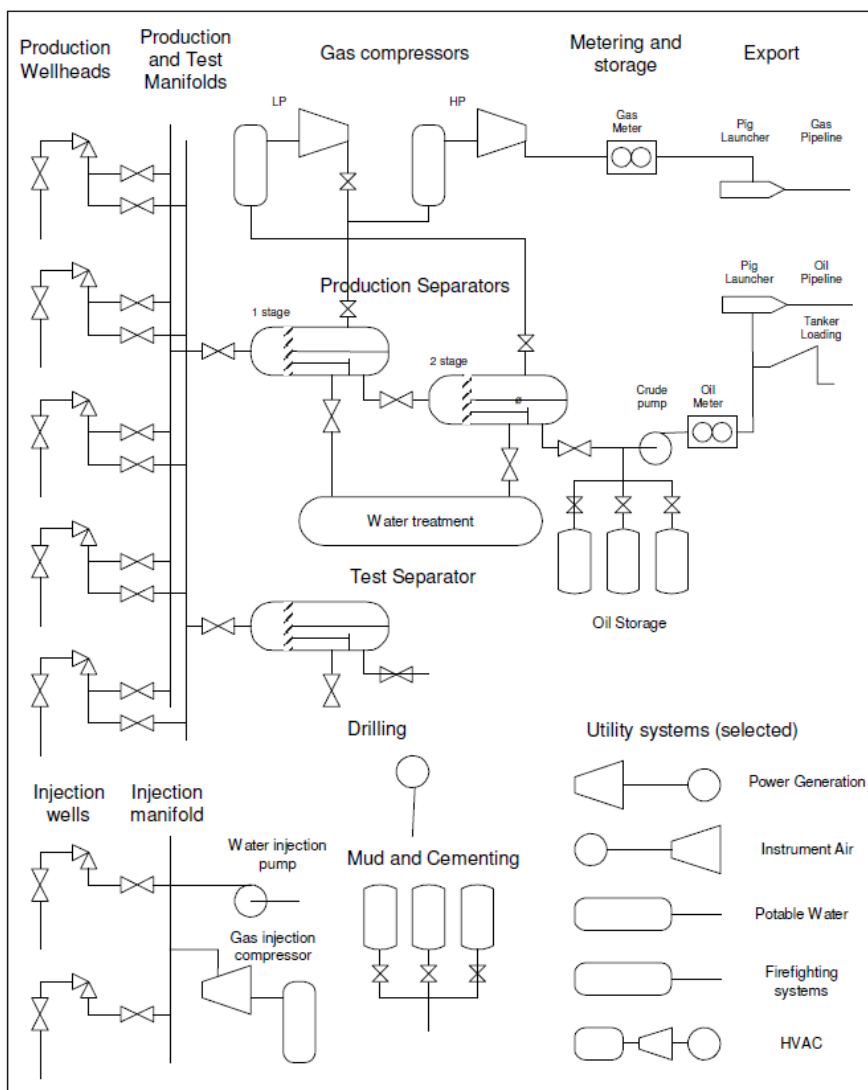
Gambar 9. 2 Ilustrasi Aplikasi IoT Migas

9.2 Pengertian Migas

Migas, singkatan dari minyak dan gas bumi, merupakan sumber daya alam yang ditemukan di dalam tanah. Minyak dan gas ini berperan penting sebagai bahan bakar utama global serta sebagai bahan baku untuk berbagai produk industri.



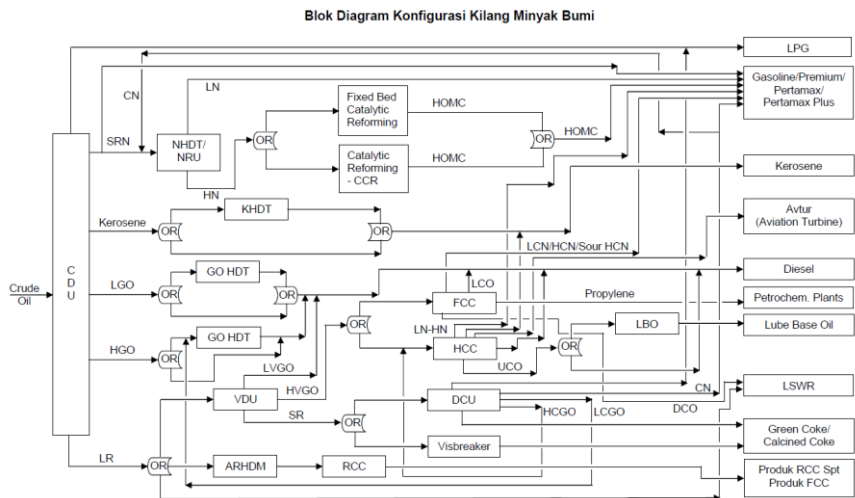
Gambar 9. 3 Sumur Minyak Sebagai Sumber Migas



Gambar 9. 4 Production Process Overview

(Sumber: Oil & Gas Production Handbook ABB)

9.3 Proses Migas



Gambar 9. 5 Diagram Alir Proses Minyak Bumi Menjadi Produk Siap Pakai

9.4 Klasifikasi Produk Industri Migas

Industri migas memproduksi berbagai jenis produk yang berperan penting dalam kehidupan sehari-hari serta berbagai sektor industri. Berikut beberapa klasifikasi produk tersebut:

- 1) Minyak Bumi (*Crude Oil*)
Produk utama dari kegiatan eksplorasi migas, minyak bumi digunakan sebagai bahan bakar utama sekaligus sebagai menjadi bahan baku dalam pembuatan berbagai produk kimia.
- 2) Gas Alam
Sebagai sumber energi bersih, gas alam dimanfaatkan dalam pembangkit listrik, pemanasan rumah, dan sebagai bahan baku industri.
- 3) Bahan Bakar Bensin dan Solar
Bensin dan solar yang dihasilkan dari pemrosesan minyak bumi, merupakan jenis bahan bakar kendaraan yang paling umum digunakan.

4) LPG (*Liquefied Petroleum Gas*)

LPG, yang berasal dari gas alam atau hasil samping pemrosesan minyak bumi, digunakan sebagai bahan bakar cair untuk keperluan rumah tangga dan industri.

5) Produk Turunan

Selain bahan bakar, industri migas juga memproduksi berbagai produk turunan, seperti aspal, pelumas, dan bahan kimia yang digunakan dalam proses manufaktur.

Tak hanya menjadi tulang punggung perekonomian global, industri migas juga berperan penting dalam memenuhi kebutuhan energi masyarakat. Sebagai salah satu pemain utama di industri ini, Indonesia terus berupaya mengoptimalkan pemanfaatan sumber daya alam demi keberlanjutan dan kesejahteraan nasional.

9.5 IoT Untuk Industri Migas

Dalam sistem IoT, komponen yang digunakan tidak jauh berbeda dengan aplikasi industri lainnya di luar migas. Alat ukur, sensor, *controller*, dan *microcontroller* tetap memiliki fungsi serta prinsip kerja yang sama. Perbedaannya terletak pada kelas peralatan yang disesuaikan dengan standar seperti *marine class* dan *oil & gas class*. Standarisasi ini bertujuan untuk memastikan keandalan peralatan agar tidak mudah rusak serta mencegah potensi kerugian, ledakan, atau kebakaran.

Komponen IoT dalam Industri Migas

1. *Hardware*

Perangkat keras yang digunakan dalam IoT migas harus memenuhi standar keamanan tinggi untuk mencegah risiko ledakan dan kebakaran akibat kegagalan perangkat. Standar keselamatan dalam pemilihan perangkat keras mencakup NFPA 70 (*Na National Electrical Code*), NFPA 497 untuk klasifikasi lokasi berbahaya, serta ATEX Standard (*Atmosphères Explosibles*).

2. *Software*

Perangkat lunak yang digunakann dapat berupa software berbayar maupun open-source, tergantung pada kebutuhan dan skala industri.

3. *Controller*

Sistem IoT migas menggunakan berbagai jenis *controller*, seperti *PLC (Programmable Logic Controller)*, *sensor*, *microcontroller*, serta perangkat komputer pendukung seperti *router*, *transmitter*, dan *receiver*.

4. *Web Service*

Web service dalam IoT migas memerlukan dukungan IT agar dapat diakses secara remote. Aplikasi berbasis web ini memungkinkan pengelolaan sistem secara efisien tanpa infrastruktur IT yang kompleks. Infrastruktur perangkat lunak dapat menggunakan layanan berbasis cloud seperti Microsoft Azure Cloud, yang mencakup hosting data, pembaruan perangkat lunak, dan fungsi dukungan dalam satu lisensi. *Web service* juga bersungsi sebagai platform yang mengintegrasikan basis data dan perangkat lunak, memungkinkan interoperabilitas antar sistem yang berbeda.

5. *Database*

Basis data (*database*) merupakan kumpulan data yang teorganisir dan dikelola menggunakan DBMS (*Database Management System*) untuk mendukung operasional industri migas.

6. *Data Analyzer*

Seorang *data analyst* bertanggung jawab dalam menganalisis data untuk mendukung pengambilan keputusan perusahaan. Selain itu, mereka juga merancang dan memelihara sistem data serta *database* guna memastikan efisiensi dan akurasi informasi dalam industri migas.

Pada dasarnya, sistem kontrol dan pemantauan dalam industri migas terdiri dari tiga komponen utama: pengukuran parameter sebagai input, pengaturan kontrol sebagai *input* maupun *output*, serta pemantauan (*monitoring*). Komponen-komponen ini dapat diklasifikasikan sebagai berikut:

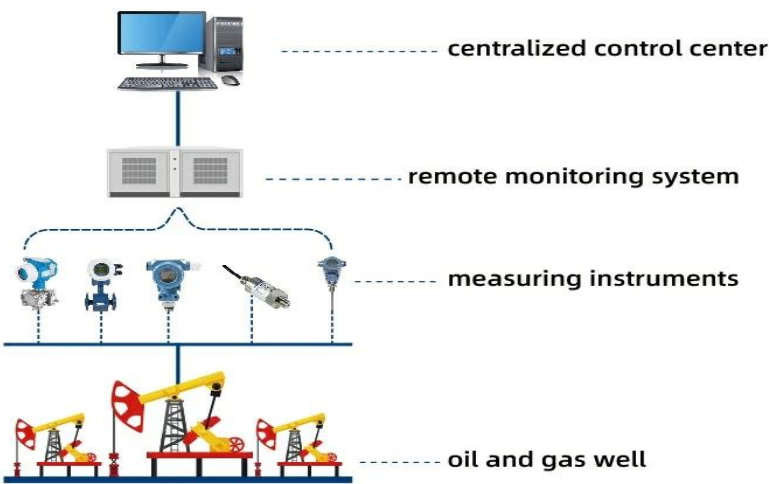
Tabel 9. 1. Parameter yang Dapat Diukur dan Dikirim dengan IoT

Pengukuran parameter	Satuan
Temperature	°C, °F
Tekanan	Bar, PSI
Level / tinggi permukaan	Meter, %
Getaran	m/sec
Waktu	min
Massa	kg
Panjang/jarak	meter
Tegangan	Volt
Arus	Ampere
Power / kWh	kW/kWh
Laju aliran massa	m ³ /h

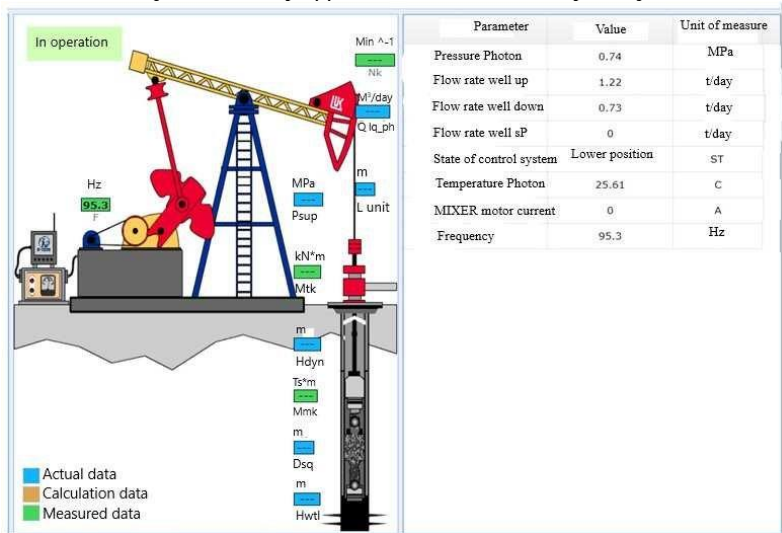
Dari berbagai jenis pengukuran tersebut, seluruh output dikirim dalam bentuk data atau signal menggunakan teknologi IOT. *Internet of Things (IoT)* dalam industri migas merupakan penerapan teknologi IoT pada sektor minyak dan gas bumi. Penggunaan IoT dalam industri ini berperan penting dalam meningkatkan efisiensi, keamanan, keselamatan kerja, serta keberlanjutan industri migas.

Beberapa contoh penerapan IoT untuk migas adalah:

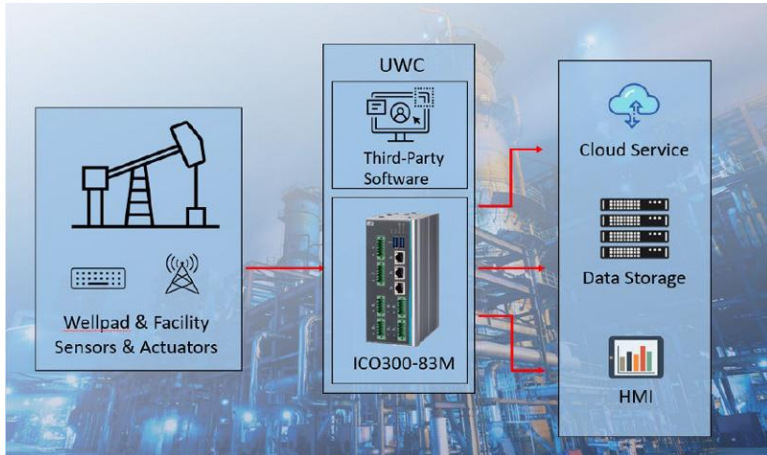
1. Pemantauan Sumur Minyak Jarak Jauh Secara *Online* dan *Real Time*



Gambar 9. 6 Diagram Proses IoT Pemantauan Sumur Migas
(Sumber: <https://www.microsensorcorp.com>)



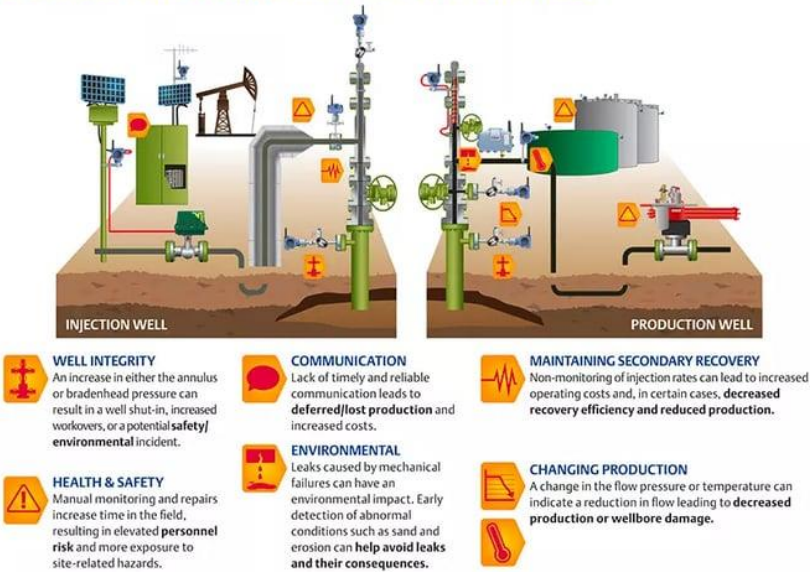
Gambar 9. 7 Tampilan IoT Dashboard Pemantauan Sumur Migas
(Sumber: Research Gate)



Gambar 9. 8 Arsitektur Sistem IoT Pemantau Sumur Migas
(Sumber: *Axiomtec*)

Saat ini, sumur minyak di ladang minyak tersebar luas dengan pemantauan dan pemeliharaan yang terbatas. Untuk memastikan operasi normal produksi, diperlukan sistem yang dapat mengirimkan informasi secara *real-time*, mencakup data produksi, status operasi pemeliharaan, cadangan minyak mentah, serta informasi transportasi. Data ini dikirim ke pusat manajemen produksi guna mendukung pengambilan keputusan yang akurat dan tepat waktu. Karena ladang minyak pada umumnya terletak di daerah terpencil, teknologi transmisi nirkabel digunakan untuk mendukung komunikasi data. Teknologi ini memiliki beberapa keunggulan, seperti instalasi yang cepat, perawatan yang mudah, biaya yang lebih rendah, serta manajemen terpusat yang efisien. (<https://www.microthings.id/>)

Common Threats to Onshore Well Performance



Gambar 9. 9 Piktorial Informasi dari Sebuah Sumur Minyak oleh IoT

(Sumber: <https://www.link-labs.com>)



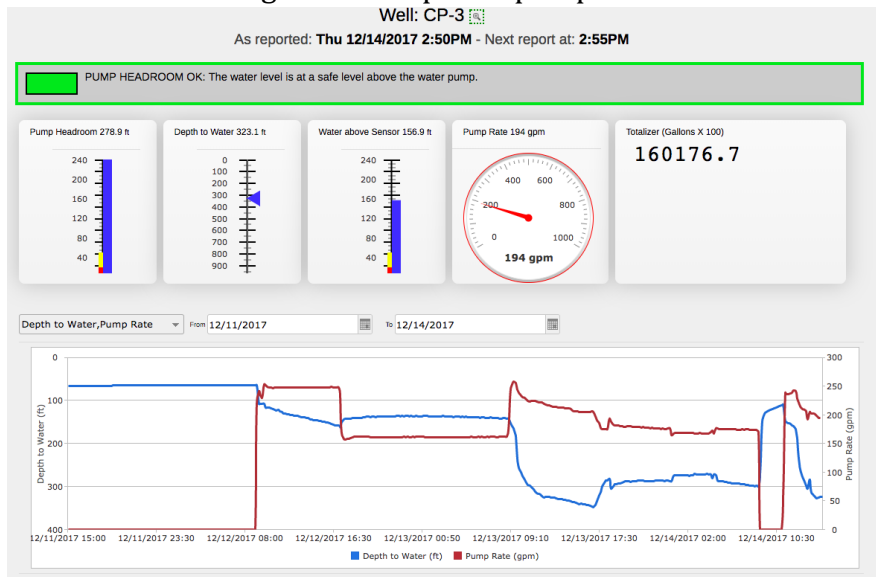
Gambar 9. 10 Aktivitas Ruang Control dan Monitoring pada Sumur Minyak

(Sumber: <https://www.aveva.com/>)

Sistem pemantauan eksplorasi minyak bekerja dengan transmisi data nirkabel menggunakan *4G Industrial IoT Edge Router R10*. Sistem ini memungkinkan pemantauan parameter sumur minyak secara *real-time*, seperti:

- Arus listrik yang digunakan oleh motor pompa
- Tegangan listrik dari sumber daya
- Temperatur pada kepala sumur
- Tekanan dalam pipa sumur
- Kecepatan dan RPM pompa

Melalui diagnosis *real-time*, sistem dapat mendeteksi kesalahan operasional, memastikan ketepatan waktu dalam pemantauan, serta memberikan alarm peringatan melalui jaringan komunikasi GPRS. Dengan teknologi ini, unit pemompaan dapat dikendalikan dari jarak jauh, termasuk untuk memulai atau menghentikan operasi pompa sesuai kebutuhan.



Gambar 9. 11 Dashboard Pemantauan Sumur

(Sumber: <https://www.valarm.net/>)

Sistem ini memerlukan sensor dan teknologi IoT untuk memungkinkan pemantauan kondisi umur minyak secara *real-time*. Beberapa parameter yang dapat dipantau meliputi:

- Suhu di berbagai titik sumur
- Tekanan dalam pipa dan kepala sumur
- Komposisi minyak mentah yang dihasilkan
- Komposisi gas yang terkandung dalam minyak
- Laju aliran minyak dan gas

Dengan pemantauan ini, sistem dapat memberikan informasi akurat dan terkini untuk meningkatkan efisiensi operasional, keamanan, serta pengellaan produksi minyak dan gas.

2. Pemantauan Tangki

Sensor IoT memungkinkan pemantauan level minyak dalam tangki penyimpanan secara real-time. Dari sisi keselamatan tangki memerlukan pemantauan temperatur dan tekanan untuk memastikan operasional tetap aman. Selain itu pemantauan visual melalui CCTV juga diperlukan untuk mengawasi kondisi eksternal tangka terkait faktor lingkungan dan keamanan. Secara khusus, IoT berfungsi sebagai berikut: [4]

- 1) Pemantauan stok - Memantau status stok di berbagai lokasi secara *real-time*.
- 2) Produktivitas dan performa aset - Sistem pemantauan stok beroperasi 24/7, memungkinkan analisis penggunaan aset berdasarkan data aktual.
- 3) Menjalankan manajemen pemeliharaan - Meningkatkan produktivitas serta mendukung pemeliharaan prediktif berdasarkan pemberitahuan dini.
- 4) Manajemen penggunaan stock – Membantu pengambilan keputusan bisnis berdasarkan *insight* data dari laporan yang tersedia.

Dengan implementasi IoT, operasional tangka penyimpanan menjadi lebih efisien, aman, dan terintegrasi, sehingga mendukung optimalisasi industri migas.

3. Pemantauan *Visual Asset*

Pemantauan asset menggunakan kamera CCTV dan *thermal camera* bertujuan untuk [5] :

1) Pemeliharaan Preventif

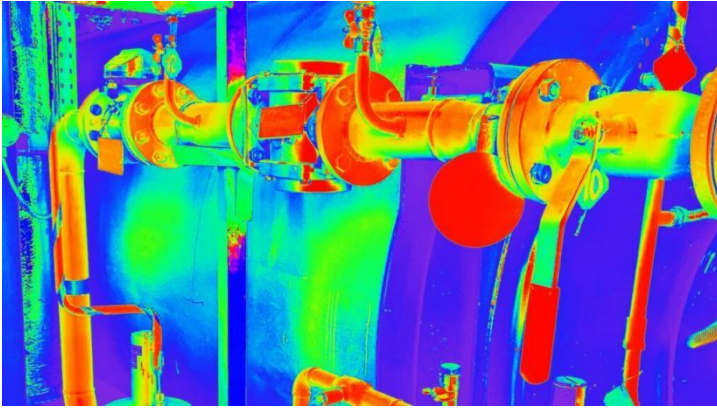
Termografi inframerah menjadi teknologi penting dalam program pemeliharaan preventif. merupakan alat yang berharga untuk program pemeliharaan preventif. Dengan melakukan pemindaian rutin pada peralatan dan infrastruktur utama, kamera pencitraan termal dapat mendeteksi potensi masalah sebelum berkembang menjadi gangguan besar. Pendekatan ini memungkinkan pencegahan gangguan operasional yang tidak terduga, memperpanjang masa pakai peralatan, serta menekan biaya perbaikan.

2) Deteksi Kebakaran

Kamera termal mampu mengidentifikasi pola panas yang tidak wajar, titik panas, atau kondisi berisiko lainnya yang dapat memicu alarm dan memberikan peringatan kepada operator mengenai potensi kebakaran. Teknologi ini berperan dalam pencegahan serta perlindungan terhadap kebakaran dengan memberikan deteksi dini, memungkinkan respons cepat, dan mengurangi risiko kebakaran besar di fasilitas minyak dan gas.

3) Keselamatan Personel

Kamera pencitraan termal berperan dalam menjaga keselamatan personel, terutama di lingkungan dengan risiko paparan suhu tinggi, seperti kilang minyak dan anjungan lepas pantai. Teknologi ini memungkinkan identifikasi titik panas, peralatan yang mengalami *overheat*, serta area dengan suhu ekstrem, sehingga operator dapat mengambil langkah pencegahan yang diperlukan untuk menghindari kecelakaan atau cedera.



Gambar 9. 12 Visualisasi Menggunakan *Thermal Camera* untuk Deteksi awal

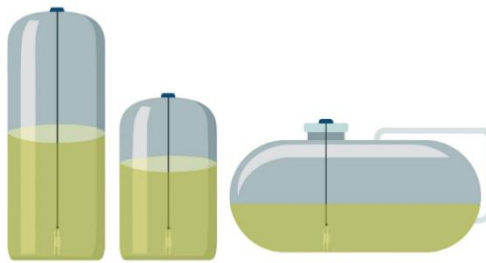
(<https://securetech.asia/thermal-cameras-in-the-oil-and-gas-industry/>)

- 4) **Pemantauan Lingkungan**
Dalam industri minyak dan gas, kamera pencitraan termal berfungsi untuk memantau serta mendeteksi potensi dampak lingkungan. Dengan mengidentifikasi perubahan suhu yang tidak biasa, seperti emisi panas berlebihan atau kebocoran, teknologi ini memungkinkan deteksi dini risiko lingkungan dan memungkinkan tindakan mitigasi segera.
- 5) **Deteksi Kebocoran**
Kamera pencitraan termal mampu mendeteksi kebocoran pada jaringan pipa dan peralatan dengan menangkap perbedaan suhu. Kebocoran cairan biasanya menyebabkan perubahan suhu di area sekitar, yang dapat divisualisasikan melalui kamera termal. Teknologi ini membantu mengidentifikasi lokasi kebocoran lebih cepat, mencegah potensi kecelakaan, serta mengurangi dampak lingkungan.
- 6) **Pemeriksaan Peralatan**
Kamera termal dapat mendeteksi pola panas yang tidak normal, sehingga membantu mengidentifikasi potensi masalah seperti motor yang mengalami *overheating*, sambungan listrik yang rusak, atau komponen yang tidak berfungsi dengan baik. Oleh karena itu, kamera ini

digunakan untuk inspeksi rutin pada peralatan seperti tangki, katup, dan pompa, memungkinkan perawatan tepat waktu, mencegah kerusakan besar, serta meningkatkan efisiensi operasional.



Gambar 9. 13 Camera Pemantau di Area Berbahaya
(Sumber: <https://www.spectrumcamera.com/>)



Gambar 9. 14 Pengukuran Ketinggian Permukaan Terhadap Tangki Minyak

(Sumber: <https://www.microsensorcorp.com/>)

Sensor-based tank monitoring, sensor pemantauan tangki berfungsi untuk emmantau kinerja serta waktu penggunaan peralatan industri migas secara real-time. Setelah mengumpulkan data, sensor akan mengirimkan informasi ke dasbor digital berbasis clous sebagai dasar untuk tindakan lanjutan atau pencegahan.

Sistem pemantauan tangki timbun menggunakan berbagai jenis sensor, seperti *level probes*, *level transmitters*, *submersible level sensors*, *contactless level sensors such as ultrasonic level sensors* dan *radar level sensors*. Sistem ini menghasilkan output berupa sinyal atau kotak.

Output digital yang tersedia dalam pemancar level pintar meliputi *RS485*, *HART*, *Long-Range Wide Area Network (LoRaWAN)* dan *modbus*. Pemancar digital ini dapat digunakan untuk mengukur level dalam berbagai jenis tangki, termasuk air, bahan bakar, dan penyimpanan. Selain itu, pemancar dengan IP 68 memiliki ketahanan terhadap korosi dan tingkat akurasi tinggi.

Sebagai contoh, sensor yang memantau persediaan minyak dalam tangki *onshore* akan otomatis mengirimkan perintah pengosongan saat tangki penuh. Sementara itu, sensor yang memantau kinerja pompa akan mengirimkan data mengenai potensi masalah kepada tim pemeliharaan jika terjadi gangguan operasional.



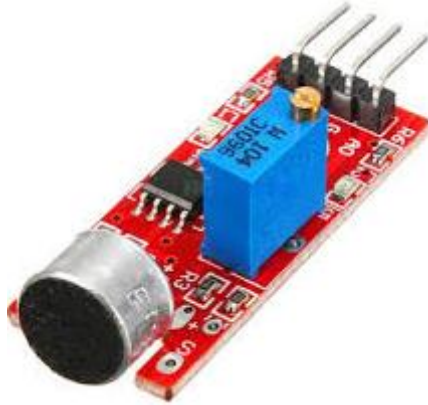
Gambar 9. 15 Recording Level Transmitter dengan Output RS485

(Sumber: <https://www.microsensorcorp.com/>)

4. Pemantauan Suara

Karena peralatan beroperasi di lokasi yang sulit dijangkau manusia, pemantauan jarak jauh yang akurat menjadi sangat penting, terutama dalam mendeteksi suara mesin selama operasional. Sensor akustik berperan dalam memantau suara

operasional peralatan untuk mengidentifikasi potensi masalah. Dengan menganalisis perubahan pola suara, sensor ini dapat mendeteksi gangguan atau kerusakan pada mesin lebih awal, memungkinkan tindakan pencegahan sebelum terjadi kegagalan yang lebih besar.



Gambar 9. 16 Sensor Suara (*Sound Sensor*)

(Sumber: Arduino.com)



Gambar 9. 17 Acoustic Sensor

(Sumber: Siemens.com)

5. Deteksi Kebocoran (*Leak Detector*)

Kebocoran dalam industri minyak dan gas merupakan kejadian berisiko tinggi yang dapat membahayakan keselamatan kerja serta menyebabkan kerugian besar. Detektor kebocoran digunakan untuk mengidentifikasi kebocoran pada pipa dan area lainnya guna memastikan keamanan serta melindungi

lingkungan kerja. Detektor ini harus mampu mendeteksi keberadaan gas yang mudah terbakar, seperti metana dan karbon monoksida, sehingga tindakan pencegahan dapat segera diambil untuk menghindari potensi bahaya.[7]



Gambar 9. 18 Gas Detector Portable Berfungsi sebagai Pengaman Pekerja yang Dapat Dikirimkan Melalui Cloud

(https://www.draeger.com/id_id/Products/Gas-Detection-Connect)

Gas Detection Connect adalah sistem yang menghubungkan pekerja dengan teknologi digital untuk meningkatkan keselamatan kerja. Sistem ini memungkinkan setiap detektor gas terintegrasi melalui perangkat lunak pintar, sehingga pemantauan dapat dilakukan kapan saja dan dari lokasi mana pun. Dengan akses *real-time*, pekerja dapat mengelola peralatan migas secara lebih efisien serta memperoleh informasi akurat mengenai posisi dan status detektor gas maupun tenaga kerja. Hal ini tidak hanya meningkatkan keselamatan, tetapi juga mengoptimalkan operasional pabrik.

Jenis detektor kebocoran gas meliputi:

- Detektor kebocoran gas ultrasonik, yang mampu mendeteksi kebocoran dengan akurasi tinggi
- Detektor gas metana, yang digunakan di kilang minyak untuk mengidentifikasi keberadaan metana, gas rumah kaca yang berkontribusi terhadap pencemaran lingkungan.
- Robot inspeksi kebocoran gas, yang dilengkapi dengan detektor metana optik dan dapat mendeteksi kebocoran pada pipa bawah tanah secara otomatis.



Gambar 9. 19 *Leak Detector Robot*

Untuk mengatasi permasalahan seperti retakan, kebocoran, dan penyumbatan pada pipa, diperlukan robot inspeksi pipa. Robot ini, khususnya robot inspeksi video, berfungsi untuk melakukan pemeriksaan pada pipa drainase secara otomatis. Dengan penerapan teknologi ini, personel pemeliharaan tidak perlu melakukan inspeksi langsung ke dalam pipa, sehingga meningkatkan efektivitas dan efisiensi pemantauan.

Inovasi ini telah menggantikan metode inspeksi manual tradisional yang kurang praktis. Selain memudahkan proses pemeriksaan, robot inspeksi pipa juga dapat mendeteksi potensi kebocoran lebih awal. Keunggulan ini menjadikannya solusi yang lebih efisien dan hemat biaya dalam perawatan sistem perpipaan.[8].

Salah satu jenis sensor ini adalah *Sensor Pellistor/Catalytic Bead*, yang bekerja dengan mendeteksi perbedaan suhu antara dua manik rangkaian. *Sensor* ini terdiri dari sepasang manik oksida logam yang dipanaskan dan ditempatkan dalam wadah tahan api. Manik-manik tersebut diletakkan pada ujung berlawanan dari rangkaian jembatan *Wheatstone*, yang bertugas mengukur perubahan resistansi listrik akibat interaksi dengan gas yang mudah terbakar[9]

(Sumber: blacklinesafety.com)

200

yang stabil. Perubahan resistansi ini diukur oleh jembatan *Wheatstone*, yang kemudian menunjukkan keberadaan gas yang mudah terbakar.

Jenis sensor untuk pemantauan keamanan di industri minyak dan gas:

1. Sensor Inframerah
 - Menggunakan cahaya inframerah untuk mendeteksi keberadaan gas berbahaya
 - Dibutuhkan untuk pemantauan jarak jauh, terutama di lingkungan yang berisiko tinggi bagi pekerja
2. Sensor Titik
 - Digunakan untuk melacak laju aliran, tekanan, suhu, dan karakteristik produk bagi titik tertentu
3. Sensor IoT untuk Prediksi Kerusakan
 - Memantau beban kerja mesin, seperti arus motor, suhu panel, tegangan sumber, vibrasi, dan RPM.
 - Memprediksi kemungkinankerusakan peralatan dan menjadwalkan perawatan preventif untuk mencegah kegagalan sistem.
4. Sistem Kendali Keamanan
 - Dapat mendeteksi gas beracun, gas yang mudah terbakar, serta percikan api.
 - Faktor yang memengaruhi deteksi ini termasuk kondisi operasional dan lingkungan kerja.
5. Manajemen Rantai Pasokan dengan Sensor IoT
 - Memantau informasi terkait jumlah minyak dan gas di lokasi klien, jumlah penggunaan, tekanan, suhu, waktu kerja, lokasi tempat kerja, nama pekerja, dan volume produksi.
 - Memungkinkan pengelolaan rantai pasokan yang lebih efisien dan terintegrasi.

6. *Acoustic Operations Monitoring*

Sistem pemantauan akustik menggunakan sensor seperti mikrofon atau hidrofون untuk merekam suara, yang kemudian dianalisis untuk mendeteksi anomali atau mengidentifikasi pola tertentu.

Sensor ini bekerja untuk mengukur komposisi oli dan laju alirannya guna mengurangi penggunaan alat-alat bernilai mahal. Dalam praktiknya, teknologi ini terus-menerus menganalisis komposisi minyak, termasuk minyak, air, gas, dan elemen lainnya di dalam pipa. Teknik pemantauan akustik pasif memanfaatkan emisi akustik (AE) yang dihasilkan oleh tumbukan partikel, terutama dengan permukaan bagian dalam dinding bejana atau pipa, sehingga memungkinkan deteksi dini terhadap potensi kerusakan atau kebocoran.[10]

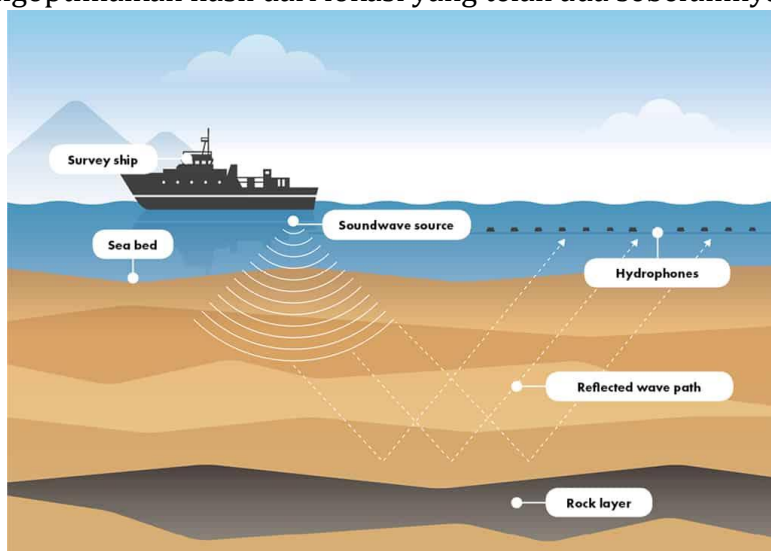
Di saat yang sama, tes laboratorium yang menyimulasikan kondisi lapangan serta penggunaan sensor terpilih dengan kinerja aliran air optimal akan memperkuat hasil pembacaan atau interpretasi sensor, memastikan keakuratan dan efektivitas sistem pemantauan.



Gambar 9. 21 Aplikasi Sensor Akustik pada Instalasi Migas

7. *Seismic Exploration Sensors*

Jaringan Sensor Nirkabel untuk Eksplorasi Seismik 3D merupakan jaringan berskala besar dan jangka panjang untuk memastikan resolusi tinggi dalam pemetaan seismik. Keseimbangan energi dalam jaringan ini sangat penting untuk menghindari gangguan yang dapat memengaruhi keseluruhan sistem[11]. gelombang seismik, yaitu gelombang elastik yang merambat di dalam bumi, perlu diukur secara akurat guna menjamin keselamatan operasional serta perlindungan terhadap infrastruktur produksi migas. Pengukuran ini dilakukan dengan sensor seismik yang berfungsi sebagai pemetaan lokasi pengeboran atau eksplorasi minyak. Sensor ini terkoneksi langsung dengan kabel serat optik bawah laut, sehingga dapat memetakan lokasi baru pengeboran bawah laut sekaligus mengoptimalkan hasil dari lokasi yang telah ada sebelumnya.



Gambar 9. 22 Aplikasi Sensor Seismik Bawah Laut

(Sumber: <https://energyproducers.au/>)

Perangkat teknologi ini juga mampu mengumpulkan hingga satu juta pembacaan per situs di internet serta men-*transfer* gambar-gambar bawah laut ke server pusat. Proses ini bertujuan untuk menganalisis data komparatif guna menentukan lokasi

pengeboran terbaik, sehingga eksplorasi dapat dilakukan dengan lebih efisien dan akurat.

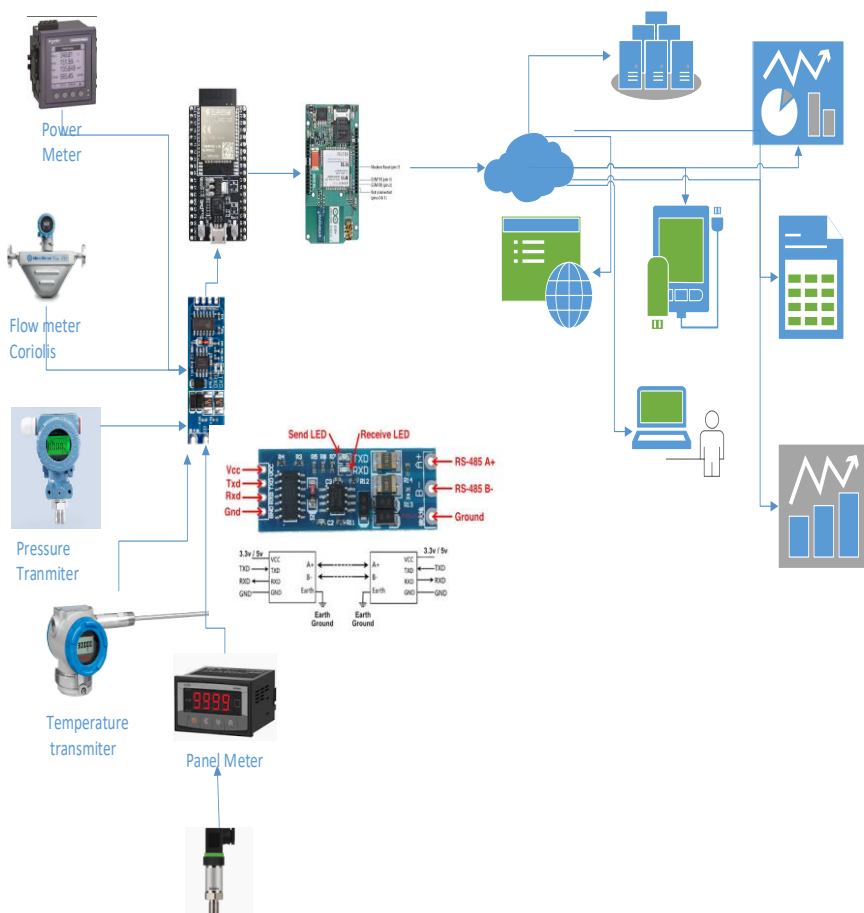
6. *Aplikasi IoT Industri Hilir Migas Computerized Gas Consumption Monitoring System dalam Industri Compressed Natural Gas (CNG)*

Compressed natural gas atau CNG adalah gas alam yang dikompresi ke dalam tabung bertekanan sebagai unit penyimpan energi. Proses kompresi dan distribusi memerlukan *control* dan *monitoring* untuk memastikan efisiensi dalam kompresi, distribusi, dan penggunaan bahan bakar. Pada setiap tahapan proses, seluruh aktivitas mesin akan selalu dikontrol dan dimonitor sesuai dengan parameter masing masing. Data yang diperoleh kemudian dikirim melalui sistem IoT ke *web server cloud*, di mana data tersebut data akan diolah dan di analisis sesuai kebutuhan, seperti untuk akuisisi data, pemantauan, serta sebagai acuan data acuan dalam perencanaan pemeliharaan.



Gambar 9. 23 *Computerized Gas Monitoring System (CGMS)*

(Sumber: Dokumen Pribadi)



Gambar 9. 24 Aplikasi IoT-Microcontroller pada CGMS

Pada aplikasi IoT di sisi distribusi gas, peran IoT sangat penting dalam perencanaan, pelaksanaan, pemantauan, dan evaluasi proses produksi serta distribusi. Selain itu, IoT juga dapat digunakan untuk membuat perkiraan (*forecast*) dan perhitungan profit perusahaan. Dengan penerapan teknologi ini, pengendalian kualitas, efisiensi, produktivitas, serta keselamatan kerja dalam rantai pasok distribusi energi migas dapat lebih terjamin

9.6 Penutup

Keberadaan IoT sangat bermanfaat dalam industri migas. Jika terjadi kondisi alarm pada operasi mesin, data alarm akan dikirim ke *cloud*, dan diteruskan ke sistem pemantauan untuk memberikan peringatan segera ke personel terkait. Salah satu manfaat penting lainnya dari penggunaan sistem IoT adalah pemeliharaan prediktif, di mana monitor IoT memantau kesehatan peralatan serta menetapkan ambang batas peringatan dan alarm. Selain itu, IoT memungkinkan peningkatan dan optimalisasi produksi dengan mengandalkan teknologi canggih seperti pembelajaran mesin (*deep learning/machine learning*) dan kecerdasan buatan (*artificial intelligence*).

Namun, penerapan IoT dalam industri migas memiliki tantangan tersendiri. Lokasi operasional yang jauh dari jangkauan manusia dan kondisi lingkungan yang berbahaya menjadi hambatan utama. Integrasi data juga menjadi tantangan dalam implementasi IoT, terutama karena keterbatasan sumber daya manusia dalam memahami integrasi sistem ini. Selain itu, diperlukan metode yang dapat diandalkan untuk menguji perangkat, memastikan *firmware* selalu diperbarui, dan melakukan instalasi jika diperlukan.

Setiap, gangguan atau kerusakan pada sistem Industrial *Internet of Things* (IIoT) dapat menyebabkan risiko fatal atau kerugian finansial yang signifikan. Salah satu risiko terbesar dalam penerapan IoT adalah keamanan data, yang rentan terhadap serangan siber. Oleh karena itu, para profesional IT harus mampu mengembangkan sistem keamanan berlapis atau *cyber security* untuk melindungi sistem IoT dari ancaman peretasan dan menjamin keandalannya.

DAFTAR PUSTAKA

- [1] K. E. Agus Salim, Biro Hukum dan Humas, "Pengusahaan Migas di Indonesia dalam Perspektif Kedaulatan Negara Atas SDA." [Online]. Available: [https://www.esdm.go.id/id/media-center/arsip-berita/pengusahaan-migas-di-indonesia-dalam-perspektif-kedaulatan-negara-atas-sda-1-pendahuluan#:~:text=Bahan galian minyak dan gas,sebagai penyumbang terbesar penerimaan negara.](https://www.esdm.go.id/id/media-center/arsip-berita/pengusahaan-migas-di-indonesia-dalam-perspektif-kedaulatan-negara-atas-sda-1-pendahuluan#:~:text=Bahan%20galian%20minyak%20dan%20gas,sebagai%20penyumbang%20terbesar%20penerimaan%20negara.)
- [2] N. Bist, S. Panchal, R. Gupta, A. Soni, and A. Sircar, "Digital transformation and trends for tapping connectivity in the oil and gas sector," *Hybrid Adv.*, vol. 6, no. February, p. 100256, 2024, doi: 10.1016/j.hybadv.2024.100256.
- [3] "Gas acousti Connect." [Online]. Available: https://www.draeger.com/id_id/Products/Gas-Detection-Connect
- [4] T. ENTERPRISE, "IoT INTANK." [Online]. Available: <https://www.telkomsel.com/enterprise/product-list-iot/iot-intank>
- [5] Miquelaa Fernando, "Thermal Cameras in the Oil and Gas Industry," Singapore, 2023. [Online]. Available: <https://securetech.asia/>
- [6] K. M. Abubeker and A. Nuthalapati, "ScienceDirect Cloud Based LoRaWAN Enabled Water Tank Automation Framework," *Procedia Comput. Sci.*, vol. 252, pp. 768–775, 2025, doi: 10.1016/j.procs.2025.01.037.
- [7] B. University, "Aplikasi IoT dalam Industri Minyak dan Gas Bumi - Graduate Program," Binus Graduate Programe. [Online]. Available: <https://graduate.binus.ac.id/2020/12/01/aplikasi-iot-dalam-industri-minyak-dan-gas-bumi/>
- [8] easysight, "CCTV Inspection Robot." Accessed: Feb. 13, 2025. [Online]. Available:

<https://www.pipedetect.com/products/pipe-inspection-robot>

- [9] Blackline safety, "Pellistor (Catalytic Bead) Sensor Technical Notes." Accessed: Feb. 13, 2025. [Online]. Available:
<https://support.blacklinesafety.com/articles/pellistor-catalytic-bead-sensors>
- [10] M. Tramontana, A. Gachagan, A. Nordon, D. Littlejohn, R. O'Leary, and A. J. Mulholland, "System modelling and device development for passive acoustic monitoring of a particulate-liquid process," *Sensors Actuators, A Phys.*, vol. 228, pp. 159–169, 2015, doi: 10.1016/j.sna.2015.03.022.
- [11] X. Zhou, J. Zheng, X. Meng, G. Sun, and R. Tian, "Design of the energy-balanced wireless sensor networks for 3D seismic exploration," *ICT Express*, vol. 9, no. 3, pp. 459–465, 2023, doi: 10.1016/j.icte.2022.04.010.

BAB 10

IMPLEMENTASI IOT PADA BIDANG TRANSPORTASI DAN *HEALTHCARE*

Oleh Fitri Puspasari

10.1 Pendahuluan

Internet of Things (IoT) ialah teknologi inovatif yang sedang berkembang pesat. Teknologi tersebut berpotensi mengubah cara manusia berinteraksi dengan lingkungan di sekitarnya. Perkembangan teknologi IoT membawa banyak perubahan diberbagai aspek kehidupan, salah satunya dibidang kesehatan. Selain itu, IoT juga mengubah industri di luar perawatan kesehatan, seperti manufaktur (Juma et al., 2023), transportasi (Jiang et al., 2023), dan pertanian (Chang et al., 2021). Oleh karena itu, penting untuk selalu mengikuti perkembangan terbaru di bidang yang menarik ini dan mengeksplorasi cara-cara IoT dapat dimanfaatkan untuk perubahan positif. Dengan IoT, berbagai perangkat mampu terhubung satu sama lain, serta mengirimkan data secara real-time, sehingga lebih efisien dan efektifif dalam operasional sehari-hari (Dang et al., 2023; Mansour et al., 2023).

Industri perawatan kesehatan merupakan salah satu sektor yang diharapkan akan memperoleh manfaat besar dari pertumbuhan ini. IoT melibatkan interkoneksi berbagai jenis subjek fisik, jenis peralatan, dan sensor melalui Internet, yang dapat dimanfaatkan sebagai alat untuk berkomunikasi satu sama lain dan berbagi data. Dalam sektor kesehatan, IoT telah mengubah cara layanan medis. Teknologi ini memungkinkan

pemantauan pasien secara jarak jauh melalui perangkat *wearable* dan sensor medis, mendukung layanan telemedicine yang lebih praktis, serta meningkatkan efisiensi manajemen rumah sakit dengan sistem otomatisasi yang lebih cerdas. Dengan IoT, tenaga medis dapat mengakses data pasien secara real-time, sehingga diagnosis dapat dilakukan lebih cepat dan perawatan menjadi lebih tepat sasaran. Selain itu, teknologi ini juga membantu mengurangi beban operasional rumah sakit, menekan biaya perawatan, serta mempercepat respons dalam situasi darurat. Seiring dengan terus berkembangnya teknologi, peran IoT dalam transportasi dan kesehatan akan semakin penting, menciptakan sistem yang lebih aman, efisien, dan berorientasi pada kebutuhan masyarakat.

Dalam dunia transportasi, teknologi ini membantu mengelola lalu lintas dengan lebih baik, mendukung pengembangan kendaraan otonom, meningkatkan pemantauan armada, serta menyediakan solusi parkir cerdas dan navigasi yang lebih akurat. Dengan memanfaatkan sensor dan sistem komunikasi canggih, IoT berkontribusi dalam mengurangi kemacetan, meningkatkan keselamatan berkendara, serta memaksimalkan penggunaan infrastruktur transportasi.

10.2 Penerapan IoT dalam Transportasi Cerdas

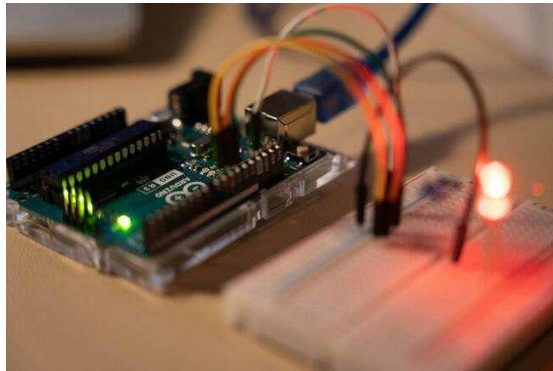
Penerapan *Internet of Things* (IoT) dalam transportasi cerdas telah membawa banyak perubahan dalam cara sistem transportasi dikelola dan dioperasikan. Dengan teknologi ini, berbagai perangkat seperti sensor, kamera, dan sistem komunikasi dapat saling terhubung untuk mengumpulkan serta menganalisis data secara real-time. Hasilnya, lalu lintas dapat diatur lebih efisien, kemacetan dapat dikurangi, dan keselamatan berkendara semakin meningkat.

IoT juga berperan penting dalam pengembangan kendaraan otonom, pemantauan armada logistik, serta solusi parkir pintar yang memudahkan pengemudi dalam menemukan tempat

parkir. Dengan terus berkembangnya teknologi ini, transportasi menjadi lebih terintegrasi, efisien, dan ramah lingkungan, sehingga memberikan manfaat besar bagi masyarakat dan industri di masa depan. Berikut adalah beberapa aplikasi IoT dalam transportasi cerdas:

10.2.1 Manajemen Lalu Lintas

Sensor IoT berperan penting untuk mengumpulkan data *real-time* mengenai kondisi lalu lintas, misalnya volume kendaraan, kecepatan rata-rata, dan kepadatan di berbagai ruas jalan. Data ini dianalisis untuk mengoptimalkan pengaturan lampu lalu lintas secara adaptif, sehingga dapat menyesuaikan durasi nyala lampu berdasarkan kondisi aktual di setiap persimpangan. Implementasi sistem ini telah terbukti mengurangi kemacetan dan meningkatkan efisiensi aliran lalu lintas.



Gambar 10. 1 Simulasi Sistem Pengendalian Lalu Lintas Berbasis IoT

(Sumber : pexels.com)

10.2.2 Kendaraan Otonom dan Terhubung

IoT memungkinkan kendaraan untuk berkomunikasi satu sama lain (*Vehicle-to-Vehicle*) dan dengan infrastruktur jalan (*Vehicle-to-Infrastructure*). Komunikasi ini

memungkinkan pertukaran informasi seperti posisi, kecepatan, dan kondisi jalan, yang berkontribusi pada peningkatan keselamatan dan efisiensi berkendara. Selain itu, kendaraan otonom memanfaatkan sensor IoT seperti radar, dan kamera untuk memantau lingkungan sekitar dan membuat keputusan berkendara secara mandiri.



Gambar 10. 2 Sistem Navigasi dan Pemantauan Penerbangan Berbasis IoT
(Sumber : pexels.com)

10.2.3 Sistem Pemantauan Armada (*Fleet Management*)

Perusahaan logistik dan transportasi memanfaatkan IoT untuk memantau armada kendaraan mereka secara *real-time*. Dengan memasang perangkat GPS dan sensor pada kendaraan, operator dapat melacak lokasi, kecepatan, konsumsi bahan bakar, dan kondisi mesin. Data ini memungkinkan pengoptimalan rute, penjadwalan pemeliharaan preventif, dan peningkatan efisiensi operasional secara keseluruhan.

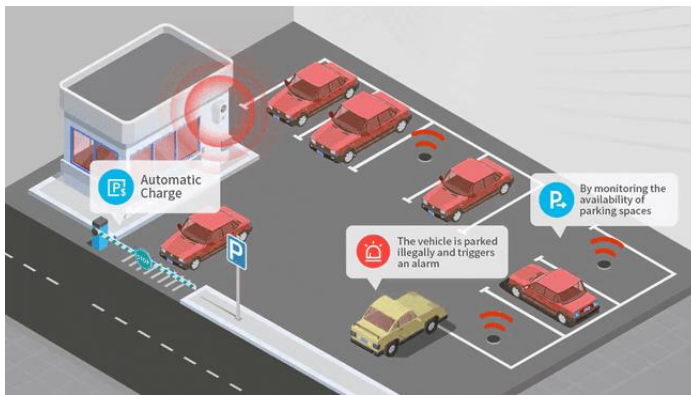


Gambar 10. 3 Teknologi IoT dalam Sistem Pemantauan Armada
(Sumber : pexels.com)

10.2.4 Smart Parking dan Navigasi *Real-Time*

Sistem parkir pintar menggunakan sensor IoT yang dipasang di tempat parkir untuk mendeteksi ketersediaan slot secara *real-time*. Informasi ini kemudian disampaikan kepada pengemudi melalui aplikasi seluler atau papan informasi digital, membantu mereka menemukan tempat parkir dengan lebih cepat dan efisien. Implementasi smart parking tidak hanya mengurangi waktu pencarian parkir,

tetapi juga mengurangi kemacetan dan emisi kendaraan di area perkotaan.



Gambar 10. 4 Teknologi IoT dalam Sistem Sistem Parkir Pintar
(Sumber : www.dusuniot.com)

10.3 IoT dalam *Healthcare*

IoT dalam bidang kesehatan membawa perubahan signifikan, teknologi ini dapat digunakan untuk memantau pasien jarak jauh, perawatan yang lebih personal, serta efisiensi dalam sistem kesehatan. Diperkirakan ada lebih dari 75 miliar perangkat IoT yang terhubung pada 2025, dengan sektor kesehatan menjadi salah satu bidang utama yang mendapatkan manfaat (Li et al., 2024).

10.3.1 Aplikasi IoT dalam *Healthcare*

Teknologi *Internet of Things* (IoT) telah banyak dimanfaatkan dalam dunia kesehatan dengan menghadirkan sistem layanan medis yang lebih efisien dan responsif. Berikut adalah beberapa contoh aplikasi IoT dalam bidang pelayanan kesehatan.

1. Pemantauan Pasien Jarak Jauh (*Remote Patient Monitoring*)

Pemantauan pasien jarak jauh adalah salah satu aplikasi utama IoT dalam layanan kesehatan. Hal tersebut memungkinkan tenaga medis untuk memantau kondisi pasien secara real-time menggunakan perangkat *wearable* dan sensor medis. Teknologi ini sangat bermanfaat bagi pasien dengan penyakit kronis, seperti diabetes dan hipertensi, karena memungkinkan pemantauan kontinu tanpa harus sering berkunjung ke rumah sakit.

IoT menggunakan cloud computing untuk menyimpan dan menganalisis data pasien. Dengan adanya integrasi AI, sistem ini mampu mendeteksi anomali dalam data kesehatan pasien dan mengirimkan notifikasi dini kepada tenaga medis jika terjadi kondisi darurat.

Beberapa contoh teknologi yang digunakan dalam pemantauan pasien jarak jauh :

a. Sensor fisiologis

Memantau tanda-tanda vital seperti denyut jantung, tekanan darah, dan kadar oksigen.

b. *Wearable health monitors*

Smartwatch dan gelang kesehatan yang mengirimkan data ke cloud untuk dianalisis.



Gambar 10.5 *Smartwatch*

(Sumber : pexels.com)

c. *Telemedicine platforms*

Pasien dapat berkonsultasi dengan dokter secara virtual, berdasarkan data yang dikumpulkan dari perangkat IoT.

d. Pemantauan pasien jarak jauh terbukti mengurangi tingkat rawat inap dan meningkatkan efektivitas perawatan pasien, terutama untuk orang-orang yang hidup di daerah terpencil.

2. ***Wearable Devices dan Sensor Medis***

Perangkat *wearable* adalah salah satu inovasi terbesar dalam IoT untuk kesehatan. Teknologi ini mencakup perangkat yang dapat dipakai pasien untuk mengukur berbagai parameter kesehatan seperti:

a. Denyut jantung dan tekanan darah misalnya menggunakan ECG monitor, *smartwatches*.



Gambar 10. 6 ECG Monitor
(Sumber : Canva.com)

- b. Kadar oksigen dalam darah (*pulse oximeter*)



Gambar 10. 7 Oximeter

(Sumber : pexels.com)

- c. Glukosa darah untuk penderita diabetes (sensor glukosa non-invasif).



Gambar 10. 8 Glucometer

(Sumber : unsplash.com)

- d. Kualitas tidur dan aktivitas fisik (*fitnes tracker, smart ring*)

3. *Telemedicine* dan Diagnostik Digital



Gambar 10. 9 Layanan Telemedicine

(Sumber : pexels.com)

IoT telah merevolusi layanan telemedicine, memungkinkan pasien untuk mendapatkan diagnosis dan perawatan jarak jauh tanpa harus mengunjungi fasilitas kesehatan. Teknologi ini semakin banyak digunakan dalam menangani pasien dengan kondisi kronis, manajemen pasien lansia, dan bahkan dalam situasi darurat seperti pandemi COVID-19. Fitur utama telemedicine berbasis IoT diantaranya ialah :

- a. *Konsultasi virtual*: Pasien dapat berkomunikasi dengan dokter melalui video call yang didukung data real-time dari perangkat wearable mereka.
- b. *AI-assisted diagnostics*: AI menganalisis gejala berdasarkan data IoT, memberikan rekomendasi medis awal sebelum pasien berkonsultasi dengan dokter.



Gambar 10. 10 Layanan *Telemedicine*
(Sumber : OpenAI)

- c. *Automated medication reminders*: Sistem IoT dapat mengingatkan pasien untuk mengonsumsi obat sesuai jadwal yang diresepkan.

4. Manajemen Rumah Sakit Berbasis IoT

IoT juga berperan dalam meningkatkan efisiensi manajemen rumah sakit dengan beberapa aplikasi berikut:

- a. Pelacakan alat medis
Sensor IoT membantu rumah sakit melacak lokasi peralatan medis seperti kursi roda, alat bedah, dan ventilator, sehingga dapat digunakan dengan lebih efisien.
- b. Manajemen tempat tidur
Sistem IoT dapat mendeteksi tingkat okupansi tempat tidur pasien dan mengoptimalkan alokasi ruangan bagi pasien baru.
- c. Otomatisasi administrasi obat
IoT membantu mengurangi kesalahan dalam pemberian obat dengan mendukung sistem pengingat otomatis untuk tenaga medis dan pasien.

10.3.2 Integrasi IoT dalam Healthcare dan Transportasi

Internet of Things (IoT) telah merevolusi berbagai sektor, termasuk kesehatan (*healthcare*) dan transportasi. IoT memungkinkan komunikasi antara perangkat fisik, sensor, dan sistem berbasis internet untuk meningkatkan efisiensi dan kualitas layanan. Contoh penerapan integrasi IoT dalam bidang Kesehatan dan transportasi misalnya ambulans pintar, IoT memungkinkan ambulans mengirim data pasien secara *real-time* ke rumah sakit untuk persiapan perawatan sebelum pasien tiba. IoT membawa transformasi besar dalam sektor kesehatan dan transportasi dengan meningkatkan efisiensi, kualitas layanan, dan keamanan. Namun, tantangan dalam hal keamanan data dan interoperabilitas masih perlu diatasi untuk mencapai implementasi yang optimal (Li et al., 2024).

DAFTAR PUSTAKA

- Dang, V. A., Khanh, Q. V., Nguyen, V., Nguyen, T., & Nguyen, D. C. (2023). Intelligent Healthcare : Integration of Emerging Technologies.
- Jiang, H., Li, X., Mahapatra, R. P., & Poovendran, P. (2023). RETRACTED ARTICLE: Creating a ubiquitous learning environment using IoT in transportation. *Soft Computing*, 27(2), 1213. <https://doi.org/10.1007/s00500-021-06018-3>
- Juma, M., Alattar, F., & Touqan, B. (2023). Securing Big Data Integrity for Industrial IoT in Smart Manufacturing Based on the Trusted Consortium Blockchain (TCB). *Internet of Things*, 4(1), 27–55. <https://doi.org/10.3390/iot4010002>
- Li, C., Wang, J., Wang, S., & Zhang, Y. (2024). A review of IoT applications in healthcare. *Neurocomputing*, 565(November 2023), 127017. <https://doi.org/10.1016/j.neucom.2023.127017>
- 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), 1–39. <https://doi.org/10.3390/en16083465>

BAB 11

IMPLEMENTASI IoT PADA BIDANG PERTANIAN DAN LINGKUNGAN

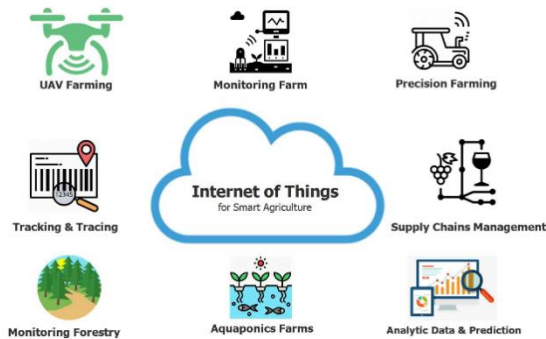
Oleh Muh. Agus

11.1 Pendahuluan

11.1.1 Peran IoT dalam Pertanian dan Lingkungan

Internet of Things (IoT) adalah sebuah revolusi teknologi yang memungkinkan perangkat untuk saling terhubung, mengumpulkan, dan berbagi data tanpa memerlukan intervensi manusia.

Dalam sektor pertanian, teknologi ini memberikan peluang optimalisasi pada berbagai proses, mulai dari penyemaian, irigasi, pemupukan, hingga distribusi hasil panen. Sebagai contoh, IoT memungkinkan pemantauan suhu tanah secara otomatis untuk menentukan waktu tanam yang paling optimal. IoT telah mengubah pendekatan dalam pengelolaan pertanian, dari metode tradisional menuju sistem berbasis data dan teknologi. Melalui sensor dan sistem yang terintegrasi, petani dapat memantau kondisi tanaman, tanah, dan lingkungan secara *real-time* untuk meningkatkan produktivitas (Quy et al. 2022).



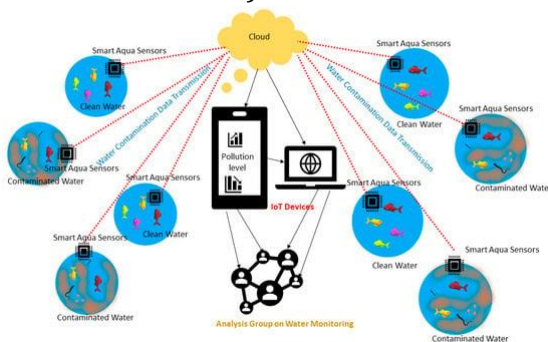
Sumber: <https://www.mdpi.com/>

Kontribusi IoT dalam Pertanian:

1. Optimalisasi Produksi: IoT mendukung peningkatan hasil panen maksimal melalui manajemen data agrikultur secara *real-time*. Contohnya adalah penggunaan drone yang dilengkapi sistem berbasis IoT untuk memantau kesehatan tanaman menggunakan citra NDVI (*Normalized Difference Vegetation Index*).
2. Keberlanjutan: Pengelolaan sumber daya seperti air dan pupuk secara terukur dapat mengurangi limbah serta dampak negatif terhadap lingkungan.

Dalam bidang lingkungan, teknologi *Internet of Things* (IoT) memainkan peran penting dalam menjaga ekosistem dengan menyediakan data *real-time* terkait kualitas udara, polusi air, dan perubahan iklim. Informasi ini sangat bermanfaat untuk mitigasi bencana dan perencanaan strategis jangka panjang. Sebagai contoh, perangkat IoT digunakan untuk memantau tingkat polutan udara seperti PM_{2.5} dan karbon monoksida (CO) di wilayah perkotaan, sehingga pemerintah dapat merumuskan kebijakan yang lebih efektif. Implementasi IoT di sektor lingkungan memberikan kontribusi signifikan dalam pengelolaan sumber daya alam, mitigasi bencana, dan pemantauan perubahan ekosistem. Contohnya adalah penggunaan sensor IoT untuk memantau kualitas air dan udara secara

real-time, serta mendeteksi perubahan lingkungan secara dini (Ullo and Sinha 2020).



Sumber: <https://www.mdpi.com/>

Kontribusi IoT pada Lingkungan:

1. **Pemantauan Kualitas Lingkungan:** IoT memungkinkan pengukuran tingkat polusi udara, seperti PM2.5, menggunakan perangkat seperti AirVisual Pro, yang membantu mengidentifikasi sumber polusi secara akurat.
2. **Peningkatan Mitigasi Bencana:** Teknologi IoT digunakan untuk mendeteksi hujan ekstrem dan pola cuaca dengan memanfaatkan *Automatic Weather Station* (AWS), yang mendukung upaya mitigasi bencana alam.

11.1.2 Pentingnya IoT untuk Pertanian dan Lingkungan

1. **Efisiensi Sumber Daya:** Teknologi IoT membantu mengurangi pemborosan sumber daya seperti air, pupuk, dan energi dengan menerapkan pengelolaan yang presisi berbasis data secara *real-time*.
2. **Keberlanjutan:** IoT mendorong penerapan praktik ramah lingkungan melalui pengelolaan sumber daya yang efisien dan berkelanjutan, sehingga dampak negatif terhadap lingkungan dapat diminimalkan.

3. Tanggap Darurat: IoT menyediakan data *real-time* yang mendukung respons cepat terhadap ancaman lingkungan, seperti bencana alam atau gangguan pada tanaman, untuk meminimalkan kerugian.

11.2 Teknologi IoT dalam Pertanian

11.2.1 Sistem Pemantauan Tanaman

Sistem Pemantauan Tanaman berbasis *Internet of Things* (IoT) adalah integrasi teknologi sensor, perangkat keras, dan jaringan internet untuk memantau kondisi pertumbuhan tanaman secara *real-time*. Sistem ini memungkinkan pengumpulan data lingkungan seperti kelembaban tanah, suhu, dan pH secara kontinu, yang kemudian dapat diakses dan dianalisis melalui platform digital. Tujuannya adalah meningkatkan efisiensi dan efektivitas dalam pengelolaan pertanian dengan menyediakan informasi yang akurat dan tepat waktu kepada petani.

Salah satu Sistem Pemantauan Tanaman yang telah dirancang oleh Agus dkk sistem yang dirancang untuk memantau kelembapan tanah, kelembapan udara, serta suhu lingkungan pada tanaman bawang merah dengan memanfaatkan teknologi IoT. Sistem ini dilengkapi dengan antarmuka aplikasi berbasis Android yang memungkinkan data sensor ditampilkan secara real-time. Empat titik kontrol terintegrasi di ladang, terhubung melalui jaringan *Wireless Sensor Network* (WSN) dengan menggunakan NodeMCU sebagai pengontrol utama Agus et al. (2023b). NodeMCU adalah platform IoT sumber terbuka. Perangkat kerasnya terdiri dari *system-on-chip* (SoC) ESP8266 yang diproduksi oleh *Espressif Systems*, dan aplikasi perangkat lunak yang menggunakan bahasa pemrograman skrip Lua (Agus et al. 2023c).

Selain itu, Doni and Rahman (2020) merancang sistem monitoring tanaman hidroponik menggunakan NodeMCU ESP8266 yang dapat memantau parameter lingkungan secara *real-time*, membantu petani dalam menjaga kondisi optimal untuk pertumbuhan tanaman.

Adapun Guntul and Agus (2021) melakukan pengembangan pada sistem berbasis IoT untuk memantau dan mengendalikan penyemprotan rumput pada tanaman padi secara otomatis maupun manual melalui perangkat Android. Sistem ini memanfaatkan NodeMCU, sensor, dan aplikasi berbasis MIT App Inventor. MIT APP Inventor merupakan platform yang digunakan untuk membuat aplikasi Android yang memungkinkan menyusun instruksi komputer dengan menyusun potongan-potongan instruksi berupa *puzzle* (Maharani et al. 2024).

Implementasi sistem pemantauan berbasis IoT ini memberikan berbagai manfaat, antara lain:

1. Pemantauan *real-time*: Memungkinkan petani untuk memantau kondisi tanaman kapan saja dan di mana saja melalui perangkat yang terhubung ke internet.
2. Pengambilan keputusan yang lebih baik: Data yang akurat membantu dalam menentukan tindakan yang tepat, seperti penyiraman atau pemupukan, berdasarkan kebutuhan aktual tanaman.
3. Efisiensi Sumber Daya: Dengan informasi yang tepat, penggunaan air dan nutrisi dapat dioptimalkan, mengurangi pemborosan dan biaya operasional.

11.2.2 Pertanian Presisi

Pertanian presisi adalah pendekatan modern dalam pertanian yang memanfaatkan teknologi untuk memberikan perlakuan spesifik sesuai kebutuhan area kecil di lahan pertanian, berbeda dengan metode tradisional yang cenderung seragam. Teknologi seperti Drone dan GPS digunakan untuk mengoptimalkan pengelolaan lahan,

meningkatkan efisiensi, dan mengurangi dampak lingkungan.

Kemajuan teknologi informasi dan telekomunikasi di bidang pertanian juga telah membawa inovasi seperti penggunaan *GPS Tracker* sebagai alat bantu navigasi. Perangkat ini memungkinkan petani melacak rute yang telah dilalui untuk menghemat bahan bakar dan mempercepat waktu perjalanan. Selain itu, *GPS Tracker* dapat memilih rute alternatif dengan dukungan sensor nirkabel. Teknologi ini, yang didukung oleh sistem satelit, memungkinkan pengiriman data terkait kecepatan, koordinat, dan arah. Analisis data ini dapat digunakan untuk mengembangkan model pengolahan lalu lintas dan menyediakan informasi tentang tingkat kepadatan jalan (Jusuf and Agus 2023).

Implementasi pertanian presisi berbasis IoT menawarkan berbagai manfaat, antara lain:

1. Efisiensi sumber daya: Penggunaan air, pupuk, dan pestisida dapat dioptimalkan berdasarkan data aktual kondisi lahan dan tanaman, sehingga mengurangi pemborosan dan dampak negatif terhadap lingkungan.
2. Peningkatan produktivitas: Dengan pemantauan yang akurat, petani dapat mengambil tindakan yang tepat waktu untuk meningkatkan hasil panen dan kualitas produk pertanian.
3. Pengambilan keputusan berdasarkan data: Data yang dikumpulkan memungkinkan analisis mendalam untuk perencanaan dan strategi pertanian yang lebih baik.

11.3.3 Otomatisasi Irigasi

Otomatisasi irigasi adalah penerapan teknologi untuk mengontrol dan mengelola sistem penyiraman tanaman secara otomatis, bertujuan meningkatkan efisiensi penggunaan air dan nutrisi serta mengoptimalkan

pertumbuhan tanaman. Dengan menggunakan sensor untuk memantau kelembaban tanah, suhu, dan parameter lingkungan lainnya, sistem ini dapat mengaktifkan atau menonaktifkan irigasi secara otomatis berdasarkan data yang diterima, sehingga penggunaan air menjadi lebih efisien. Data yang dikumpulkan dapat dikirim melalui jaringan internet ke *platform* yang dapat diakses oleh petani, yang memungkinkan mereka untuk memantau dan mengontrol irigasi dari jarak jauh.

Sistem irigasi cerdas menggunakan sensor kelembapan tanah yang terintegrasi dengan aktuator irigasi untuk memastikan tanaman mendapatkan air sesuai kebutuhan. Sistem ini, seperti yang dirancang oleh Rafrin et al. (2024), yang memanfaatkan machine learning untuk meningkatkan efisiensi pengelolaan air dalam pertanian bawang merah.

Pada sistem hidroponik, sensor TDS (*Total Dissolved Solids*) digunakan untuk mengontrol konsentrasi nutrisi, sedangkan sensor pH membantu menjaga tingkat keasaman yang optimal. Studi oleh Agus et al. (2023a) menunjukkan bahwa integrasi teknologi berbasis Arduino pada sistem hidroponik dapat meningkatkan efisiensi penggunaan air dan nutrisi serta mempermudah pengendalian hama dan penyakit. Bagian Otak yaitu berupa Arduino sebagai pengendali Aktuator berdasarkan nilai sensor (Agus et al. 2024).

Manfaat utama dari otomatisasi irigasi berbasis IoT antara lain:

1. Efisiensi penggunaan air: Dengan sistem otomatis yang dapat menyesuaikan aliran air sesuai kebutuhan tanaman, pemborosan air dapat diminimalkan.
2. Penghematan waktu dan tenaga: Otomatisasi mengurangi kebutuhan akan pengawasan dan kontrol manual terhadap sistem irigasi, mempermudah manajemen sumber daya.

3. Pemantauan jarak jauh: Petani dapat memantau kondisi irigasi dan lingkungan secara *real-time* melalui aplikasi atau perangkat yang terhubung ke internet.

11.3 Teknologi IoT dalam Lingkungan

11.3.1 Pemantauan Kualitas Udara dan Air

Pemantauan Kualitas Udara dan Air berbasis *Internet of Things* (IoT) adalah penggunaan teknologi sensor dan perangkat yang terhubung dengan internet untuk mengukur dan menganalisis parameter kualitas udara dan air secara *real-time*. Dengan sistem ini, data tentang polutan udara, seperti partikel materi (PM2.5 dan PM10), nitrogen dioksida (NO₂), sulfur dioksida (SO₂), serta kualitas air yang meliputi pH, suhu, dan kadar oksigen terlarut dapat dipantau secara otomatis. Data yang diperoleh dapat dikirim ke platform berbasis cloud dan diakses oleh pengguna melalui aplikasi atau dashboard, memungkinkan pengelolaan kualitas lingkungan secara lebih efisien dan responsif.

Pebralia et al. (2024) dalam penelitiannya tentang Implementasi *Internet of Things* (IoT) dalam Monitoring Kualitas Udara pada Ruang Terbuka mengungkapkan bahwa penerapan teknologi IoT dalam pemantauan kualitas udara di ruang terbuka dapat memberikan peringatan dini terhadap kondisi polusi yang berpotensi membahayakan kesehatan masyarakat. Sistem ini memungkinkan pengumpulan data secara real-time dan analisis untuk mengidentifikasi polusi udara serta memberikan respons yang cepat terhadap perubahan kualitas udara.

Menurut penelitian yang dilakukan oleh Yushananta (2023), platform pemantauan kualitas udara berbasis *Internet of Things* (IoT) dengan biaya sangat rendah telah dikembangkan untuk memungkinkan pemantauan kualitas udara secara real-time. Platform ini menggunakan sensor untuk mengukur parameter kualitas udara dan

mengirimkan data ke platform cloud untuk analisis lebih lanjut, memberikan solusi hemat biaya dalam memantau kualitas udara di berbagai lokasi.

Adapun penelitian yang dilakukan oleh Hidayati et al. (2024), mengembangkan sistem pemantauan kualitas udara secara *real-time* menggunakan ESP32 dan teknologi IoT. Sistem ini memungkinkan pemantauan parameter kualitas udara seperti suhu, kelembaban, dan polutan udara secara langsung melalui perangkat yang terhubung ke internet, memberikan data yang berguna untuk tindakan mitigasi terhadap polusi udara.

Manfaat utama dari pemantauan kualitas udara dan air berbasis IoT antara lain:

1. Pemantauan *real-time*: Data kualitas udara dan air dapat diperoleh secara langsung dan terus-menerus, memungkinkan respons cepat terhadap perubahan kondisi lingkungan.
2. Peningkatan kesadaran masyarakat: Dengan sistem yang terhubung ke aplikasi, masyarakat dapat mengakses informasi kualitas lingkungan di sekitar mereka, meningkatkan kesadaran tentang pentingnya menjaga kualitas udara dan air.
3. Pengelolaan lingkungan yang lebih baik: Data yang terkumpul dapat digunakan oleh pemerintah dan organisasi untuk merancang kebijakan lingkungan yang lebih efektif dan proaktif.

11.3.2 Pengelolaan Sampah Pintar

Pengelolaan Sampah Pintar berbasis *Internet of Things* (IoT) adalah sistem yang memanfaatkan teknologi IoT untuk memantau, mengelola, dan mengoptimalkan pengelolaan sampah secara efisien. Sistem ini mengintegrasikan sensor, perangkat keras, dan platform berbasis internet untuk memantau tingkat sampah dalam tempat sampah secara *real-time*, serta memberikan data

untuk pengelolaan sampah yang lebih efektif, seperti penjadwalan pengambilan sampah otomatis dan pemrosesan sampah secara lebih ramah lingkungan.

Menurut penelitian yang dilakukan oleh Muslimin et al. (2022) menyarankan penerapan *Internet of Things* (IoT) untuk sistem pembuangan akhir sampah di Mojokerto. Teknologi ini memungkinkan pemantauan status sampah di tempat pembuangan akhir (TPA) secara *real-time*, serta meningkatkan efisiensi dan transparansi dalam pengelolaan sampah.

Penelitian yang dilakukan oleh Agustino et al. (2024) menunjukkan inovasi dalam pengelolaan sampah dengan mengembangkan tempat sampah pintar berbasis IoT di Museum MH. Thamrin, Jakarta. Sistem ini memungkinkan pemantauan dan pengelolaan sampah secara otomatis, serta mendukung pengelolaan sampah yang lebih ramah lingkungan dan terkelola dengan baik.

Manfaat utama dari pengelolaan sampah pintar berbasis IoT antara lain:

1. Pengelolaan sampah yang lebih efisien: Sistem ini memungkinkan pemantauan tingkat sampah secara otomatis, yang membantu dalam merencanakan pengangkutan sampah dan mencegah penumpukan.
2. Pengurangan dampak lingkungan: Dengan sistem yang lebih efisien, jumlah sampah yang tidak terkelola dengan baik dapat dikurangi, mengurangi dampak negatif terhadap lingkungan, seperti pencemaran.
3. Peningkatan layanan masyarakat: Masyarakat dapat merasakan manfaat dari sistem pengelolaan sampah yang lebih baik, dengan pengambilan sampah yang lebih terjadwal dan lebih sedikit tumpukan sampah di area publik.

11.3.3 Pemantauan Perubahan Iklim

Pemantauan Perubahan Iklim berbasis *Internet of Things* (IoT) adalah sistem yang memanfaatkan sensor dan perangkat IoT untuk memantau parameter iklim seperti suhu, kelembaban udara, curah hujan, dan tekanan atmosfer secara *real-time*. Data yang dikumpulkan dari sensor-sensor ini dikirim ke platform berbasis internet, memungkinkan analisis data yang lebih cepat dan akurat untuk memantau tren perubahan iklim dan dampaknya terhadap lingkungan. Tujuan dari sistem ini adalah untuk mendeteksi perubahan iklim dengan lebih presisi dan menyediakan informasi yang diperlukan untuk perencanaan mitigasi serta adaptasi terhadap perubahan iklim.

Sebagai contoh, penelitian oleh Nugroho et al. (2023), stasiun pemantau cuaca berbasis *Internet of Things* (IoT) telah dirancang untuk memantau kondisi cuaca di Kabupaten Bandung. Sistem ini memungkinkan pengumpulan data cuaca secara *real-time* menggunakan berbagai sensor yang terhubung dengan platform IoT, yang kemudian dapat diakses oleh pengguna untuk analisis lebih lanjut.

Selain itu, penelitian yang dilakukan oleh Nurwasito and Adaby (2024) mengembangkan sistem IoT untuk perekaman data iklim mikro menggunakan platform Thingsboard. Sistem ini memungkinkan pemantauan kondisi iklim mikro secara *real-time*, yang dapat membantu dalam pengambilan keputusan terkait pertanian, pengelolaan lingkungan, dan penelitian cuaca.

Manfaat dari pemantauan perubahan iklim berbasis IoT antara lain:

1. Pemantauan *real-time*: Memungkinkan pengumpulan data lingkungan secara langsung, yang berguna untuk mendeteksi perubahan iklim yang cepat dan menyediakan informasi yang lebih akurat.

2. Peningkatan respons terhadap perubahan iklim: Data yang dikumpulkan dapat digunakan untuk merencanakan tindakan mitigasi, seperti pencegahan bencana alam atau pengelolaan sumber daya alam yang lebih baik.
3. Pemahaman yang lebih baik tentang dampak perubahan iklim: Sistem ini memberikan wawasan yang lebih dalam mengenai bagaimana perubahan iklim mempengaruhi berbagai aspek kehidupan, mulai dari pertanian hingga kualitas udara di perkotaan.

11.4 Keuntungan dan Tantangan Implementasi IoT

11.4.1 Keuntungan

1. Efisiensi Operasional: Mengurangi pemborosan sumber daya. Penggunaan air, pupuk, dan energi lebih hemat.
2. Keberlanjutan: Mendukung pengelolaan sumber daya alam yang lebih baik.
3. Pengambilan Keputusan Berbasis Data: Memberikan data *real-time* untuk rekomendasi terbaik. Data yang akurat untuk prediksi cuaca dan hasil panen.

11.4.2 Tantangan

1. Keterbatasan Infrastruktur: Area terpencil sering kali tidak memiliki jaringan internet memadai.
2. Biaya Implementasi: Instalasi perangkat IoT bisa menjadi beban bagi petani kecil.
3. Keamanan Data: Sistem IoT rentan terhadap serangan siber jika tidak dilengkapi enkripsi yang baik.

11.5 Studi Kasus dan Masa Depan

11.5.1 Studi Kasus dan Implementasi di Dunia Nyata

1. Pertanian: Smart farming di Belanda menggunakan teknologi IoT untuk rumah kaca otomatis.
2. Lingkungan: Sistem IoT di Tanzania untuk melindungi spesies liar dari perburuan ilegal.

11.5.2 Masa Depan IoT dalam Pertanian dan Lingkungan

1. Tren: Integrasi IoT dengan AI untuk analisis prediktif dan blockchain untuk transparansi rantai pasokan.
2. Potensi: Pemanfaatan teknologi edge computing untuk mengurangi ketergantungan pada cloud.

11.6 Praktikum IoT pada Pertanian dan Lingkungan

11.6.1 Komponen dan Alat yang Digunakan

1. **Perangkat Keras:**
 - a. Mikrokontroler: ESP32, Arduino Uno, atau Raspberry Pi.
 - b. Sensor:
 - 1) DHT22: Untuk memantau suhu dan kelembapan udara.
 - 2) Soil Moisture Sensor: Untuk mengukur kelembapan tanah.
 - 3) pH Sensor: Untuk memantau keasaman air dalam hidroponik.
 - 4) MQ-135: Untuk mendeteksi polusi udara.
 - c. Aktuator: Relay, pompa air, motor servo.
2. **Perangkat Lunak:**
 - a. Arduino IDE atau PlatformIO untuk pemrograman perangkat.
 - b. Node-RED untuk visualisasi aliran data IoT.

- c. Firebase, ThingSpeak, atau Blynk untuk penyimpanan dan pengelolaan data.
- 3. Platform Cloud:**
- a. AWS IoT Core untuk skala besar.
 - b. ThingsBoard untuk visualisasi data real-time.
 - c. Modem Wi-Fi untuk konektivitas perangkat IoT.

11.6.2 Rancangan Modul Praktikum

1. Pengenalan dan Instalasi Perangkat IoT

- a. Materi: Penggunaan board mikrokontroler (seperti Arduino atau ESP32) untuk mengakses sensor.
- b. Praktik:
 - 1) Menghubungkan sensor suhu dan kelembapan (DHT11/DHT22) ke mikrokontroler.
 - 2) Menampilkan data pada serial monitor dan LCD.
- c. Hasil: Output berupa data suhu dan kelembapan udara yang ditampilkan secara real-time pada serial monitor atau LCD.

2. Sistem Pemantauan Kelembapan Tanah

- a. Materi: Penggunaan *Soil Moisture* Sensor untuk memantau kelembapan tanah secara *real-time*.
- b. Praktik:
 - 1) Merancang sistem pemantauan kelembapan tanah yang mengirim data ke aplikasi smartphone melalui protokol MQTT.
 - 2) Mengintegrasikan data dengan Firebase untuk penyimpanan dan analisis.
- c. Hasil: Output berupa data suhu dan kelembapan udara yang ditampilkan secara real-time pada serial monitor atau LCD.

3. Implementasi Irigasi Otomatis

- a. Materi: Menggunakan aktuator seperti relay dan pompa air untuk mengotomatisasi sistem irigasi berdasarkan data sensor.
- b. Praktik:
 - 1) Membuat sistem yang mengaktifkan pompa air secara otomatis jika kelembapan tanah di bawah ambang tertentu.
 - 2) Mengatur logika kontrol menggunakan Arduino IDE atau Node-RED.
- c. Hasil: Output berupa data suhu dan kelembapan udara yang ditampilkan secara real-time pada serial monitor atau LCD.

4. Pemantauan Kualitas Udara

- a. Materi: Penggunaan sensor kualitas udara (MQ-135) untuk mendeteksi polusi udara.
- b. Praktik:
 - 1) Menampilkan data kualitas udara di dashboard IoT seperti Blynk atau ThingsBoard.
 - 2) Mengintegrasikan notifikasi otomatis ke smartphone jika tingkat polusi mencapai ambang bahaya.
- c. Hasil: Output berupa data suhu dan kelembapan udara yang ditampilkan secara real-time pada serial monitor atau LCD.

5. Pengenalan Drone IoT untuk Pertanian

- a. Materi: Menggunakan drone yang dilengkapi kamera multispektral untuk memetakan kesehatan tanaman.
- b. Praktik:
 - 1) Simulasi analisis citra menggunakan NDVI (*Normalized Difference Vegetation Index*).
 - 2) Pemrosesan data di cloud untuk menghasilkan peta lahan pertanian.

- c. Hasil: Output berupa data suhu dan kelembapan udara yang ditampilkan secara *real-time* pada serial monitor atau LCD.
- 6. Pemantauan Nutrisi pada Hidroponik dengan IoT**
- a. Materi: Penggunaan sensor TDS untuk memantau kandungan nutrisi air.
 - b. Praktik:
 - 1) Merancang sistem yang mengontrol pemberian nutrisi berdasarkan nilai TDS.
 - 2) Mengintegrasikan data ke aplikasi dashboard untuk pemantauan jarak jauh.
 - c. Hasil: Sistem hidroponik otomatis yang memastikan konsentrasi nutrisi tetap optimal.
- 7. Implementasi IoT pada Deteksi Kebakaran Hutan**
- a. Materi: Penerapan sensor suhu dan gas (seperti MQ-2) untuk mendeteksi potensi kebakaran.
 - b. Praktik:
 - 1) Membuat sistem peringatan dini dengan notifikasi SMS atau email.
 - 2) Menggunakan kamera termal untuk analisis tambahan (opsional).
 - c. Hasil: Sistem berbasis IoT yang dapat digunakan untuk mencegah penyebaran kebakaran.
- 8. Analisis Data IoT dengan Machine Learning**
- a. Materi: Pemanfaatan algoritma ML untuk prediksi pola berdasarkan data IoT.
 - b. Praktik:
 - 1) Menggunakan dataset kelembapan tanah dan curah hujan untuk memprediksi waktu penyiraman optimal.
 - 2) Menerapkan model sederhana di platform cloud (misalnya Google Cloud AI).

- c. Hasil: Peningkatan efisiensi sistem irigasi melalui prediksi berbasis data.

9. Simulasi Drone IoT untuk Pemantauan Lahan

- a. Materi: Penggunaan drone untuk survei lahan dengan perangkat IoT.
- b. Praktik:
 - 1) Simulasi penerbangan drone untuk mengambil data NDVI.
 - 2) Integrasi data dengan perangkat IoT darat untuk analisis kesehatan tanaman.
- c. Hasil: Pemetaan lahan pertanian dengan detail tinggi untuk optimasi penggunaan sumber daya.

11.6.3 Studi Kasus Praktikum

1. Proyek Mini: Sistem Irigasi Cerdas untuk Tanaman Cabai
 - a. Deskripsi: Membuat sistem irigasi yang mengontrol pemberian air berdasarkan sensor kelembapan tanah.
 - b. Langkah-Langkah:
 - 1) Pasang sensor kelembapan di dekat akar tanaman.
 - 2) Gunakan mikrokontroler untuk membaca data sensor dan mengaktifkan pompa jika kelembapan rendah.
 - 3) Kirim data ke *Firestore* dan tampilkan grafik kelembapan di aplikasi dashboard.
 - c. Hasil Akhir: Prototipe yang meminimalkan pemborosan air.
2. Proyek Mini: Pemantauan Kualitas Udara untuk Area Urban
 - a. Deskripsi: Merancang alat berbasis IoT untuk mendeteksi polusi udara di perkotaan.
 - b. Langkah-Langkah:

- 1) Gunakan MQ-135 untuk mengukur konsentrasi polutan seperti CO dan NO₂.
 - 2) Kirim data ke ThingsBoard untuk visualisasi *real-time*.
 - 3) Tambahkan fitur notifikasi ketika polusi melebihi ambang batas.
- c. Hasil Akhir: Sistem berbasis IoT yang dapat meningkatkan kesadaran publik terhadap kualitas udara.

11.6.4 Tantangan dalam Praktikum

1. Ketersediaan Alat dan Bahan: Beberapa perangkat IoT memerlukan biaya tinggi atau sulit diperoleh.
2. Koneksi Internet Terbatas: Praktikum di area terpencil memerlukan solusi alternatif seperti LoRa atau Zigbee.
3. Kesulitan Teknis: Membutuhkan pelatihan tambahan untuk mengatasi masalah perangkat keras dan perangkat lunak.

11.7 Kesimpulan

Teknologi IoT menawarkan solusi revolusioner untuk tantangan di bidang pertanian dan lingkungan. Dengan pengembangan infrastruktur jaringan dan biaya perangkat yang semakin terjangkau, adopsi IoT di masa depan akan semakin luas. Inovasi lebih lanjut, seperti integrasi AI, *blockchain*, dan IoT, diharapkan dapat meningkatkan efisiensi dan keberlanjutan sektor ini secara signifikan.

DAFTAR PUSTAKA

- Agus, Muh. et al. 2024. Pelatihan Robot Sederhana Untuk Tngkatkan Logika Berfikir Siswa di SMKN 2 Pinrang. *MONSU'ANI TANO Jurnal Pengabdian Masyarakat* 7(2), pp. 129–146.
- Agus, Muh., Akhsa, A.T.P.D. and Yunus, S.R. 2023a. Perancangan Sistem Pemberian Nutrisi Tanaman Sayuran Hidroponik Otomatis Berbasis Arduino. *Jurnal Fokus Elektroda: Energi Listrik, Telekomunikasi, Komputer, Elektronika dan Kendali* 8(4), pp. 248–258.
- Agus, Muh., Ayu Maharani, P. and Rafrin, M. 2023b. Perancangan Sistem Pemantauan Kelembaban Tanah,Udara dan Suhu pada Tanaman Bawang Merah Menggunakan IoT. *Prosiding Seminar Nasional SISFOTEK* 7(1), pp. 102–108.
- Agus, Muh., Hasyim, M.F., Erlangga, M.I. and Yunus, S.R. 2023c. Perancangan Sistem Pemberian Pakan Ayam Cerdas (SPACE) Guna Meningkatkan Produktivitas Ayam Petelur Menggunakan NodeMCU. *Konferensi Nasional Ilmu Komputer (KONIK) 2023* 7(2), pp. 129–146.
- Agustino, R., Saputro, M.I., Gustiawan, H., Sakaria, M.A. and Widyahastuti, F. 2024. Inovasi Pengelolaan Sampah: Tempat Sampah Pintar Berbasis IoT di Museum MH.Thamrin Jakarta. *Jurnal Teknologi Informatika dan Komputer* 10(1), pp. 313–3259.
- Doni, R. and Rahman, M. 2020. Sistem Monitoring Tanaman Hidroponik Berbasis Iot (Internet of Thing) Menggunakan Nodemcu ESP8266. *Jurnal Sains Komputer & Informatika (J-SAKTI)* 4(2), pp. 516–522.
- Guntul and Agus, Muh. 2021. Rancang Bangun Monitoring Penyemprotan Rumput Pada Tanaman Padi Berbasis Android. *Jurnal IT: Media Informasi STMIK Handayani Makassar* 12(1), pp. 57–67.

- Hidayati, R., Sari, K., Halawa, Y., Tafrihan, A. and Harits, M.A. 2024. Sistem Pemantauan Kualitas Udara secara Real-time Menggunakan ESP32 dan Teknologi IoT. *Djtechno : Jurnal Teknologi Informasi* 5(2), pp. 232–245.
- Jusuf, A.K. and Agus, M. 2023. Penerapan Sistem Tracking Berbasis GPS Pada Alat Pendeteksi Alkohol Terintegrasi Dengan Arduino Untuk Pengemudi Mobil Penumpang Umum. *Journal of System and Computer Engineering*.
- Maharani, P.A. et al. 2024. Pelatihan MIT App Inventor sebagai Upaya Meningkatkan Kemampuan Berpikir Logis Siswa SMAN 4 Parepare. *Jurnal Pengabdian UNDIKMA* 5(1), pp. 161–169.
- Muslimin, Moh., Andhika C.P., Ardiantoro, L. and Zahara, S. 2022. Internet of Thing (IoT) untuk Pembuangan Akhir Sampah di Mojokerto. *INSOLOGI: Jurnal Sains dan Teknologi* 1(6), pp. 897–906.
- Nugroho, T.A., Suakanto, S. and Gamaliel, Y. 2023. Stasiun Pemantau Cuaca Berbasis Internet of Things (Studi Kasus Kabupaten Bandung). 8, pp. 1–07.
- Nurwasito, H. and Adaby, R.W. 2024. Pengembangan Internet of Things (IoT) dalam Perekaman Data Iklim Mikro dengan Platform Thingsboard. *Jurnal Teknologi Informasi dan Ilmu Komputer (JTIIK)* 11(6), pp. 1385–1398.
- Pebralia, J., Akhsan, H. and Amri, I. 2024. Implementasi Internet of Things (IoT) dalam Monitoring Kualitas Udara Pada Ruang Terbuka. *Jurnal Kumparan Fisika* 7(1), pp. 1–8.
- Quy, V.K. et al. 2022. IoT-Enabled Smart Agriculture: Architecture, Applications, and Challenges. *Applied Sciences (Switzerland)* 12(7), pp. 1–19.
- Rafrin, M., Agus, Muh. and Maharani, P.A. 2024. IoT-Based Irrigation System Using Machine Learning for Precision Shallot Farming. *Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi)* 8(2), pp. 216–222.

- Ullo, S.L. and Sinha, G.R. 2020. Advances in smart environment monitoring systems using iot and sensors. *Sensors (Switzerland)* 20(11), pp. 1–18.
- Yushananta, P. 2023. Very Low-Cost, Internet of Things (IoT) Air Quality Monitoring Platform. *Jurnal Aisyah : Jurnal Ilmu Kesehatan* 8(2), pp. 441–446.

BIODATA PENULIS



Wahyuddin S., S.Kom., M.Kom

Dosen STMIK Amika Soppeng

Wahyuddin S. was born at Malaka-Bone-Sulawesi Selatan in 1992. In 2011 he attended Dipa Makassar University (UNDIPA) and was completed in 2015. He was completed after attending 7 semesters and active on an XPcom (Extreme Programmer Computer) campus organization. He was also active as a lecturer assistant for three semesters and taught several courses on programming. He continued his Master of Information systems at Indonesia Computer University (UNIKOM) Bandung in 2016 and was completed in April 2019. In 2023, he continues his doctoral studies in the computer science study program at Sepuluh Nopember Institute of Technology (ITS) Surabaya. He worked as a lecturer at a campus (STMIK Amika Soppeng) 2019 to present and also a Freelance Web Programmer. Has competence in the field of software engineer, application developer, multimedia, web developer, network security, and data analyst.

BIODATA PENULIS



Dwi Feriyanto. S.T., M.Pd.

Dosen Program Studi S1 Rekayasa Perangkat Lunak
Fakultas Teknologi dan Informatika
Universitas Aisyah Pringsewu, Lampung

Penulis lahir di Jatibaru tanggal 26 Februari 1983. Penulis merupakan Dosen pada Program Studi DIII Teknik Elektronika sampai tahun 2024, selanjutnya bertugas di Program Studi S1 Rekayasa Perangkat Lunak (RPL) Fakultas Teknologi dan Informatika Universitas Aisyah Pringsewu, Lampung. Penulis menyelesaikan pendidikan jenjang S1 pada Jurusan Teknik Elektro dan jenjang S2 pada Jurusan Pendidikan Teknik Elektro. Keahlian yang ditekuni yaitu elektronika rumah tangga, *Internet of Things* (IoT), serta instalasi penerangan dan tenaga.

BIODATA PENULIS



Dwi Sasmita Aji Pambudi, S.T., M.T.

Dosen Program Studi Teknik Kelistrikan Kapal
Politeknik Perkapalan Negeri Surabaya (PPNS)

Penulis lahir di Lumajang tanggal 21 April 1992. Penulis adalah dosen tetap pada Program Studi Teknik Kelistrikan Kapal, Jurusan Teknik Kelistrikan Kapal, Politeknik Perkapalan Negeri Surabaya (PPNS). Penulis menyelesaikan pendidikan S1 pada Jurusan Teknik Elektro di Universitas Telkom, Bandung pada tahun 2013 dan melanjutkan jenjang S2 pada Jurusan Teknik Elektro, Bidang Keahlian Elektronika di Institut Teknologi Sepuluh Nopember (ITS), Surabaya pada tahun 2018. Penulis mulai menekuni bidang menulis sejak awal menjadi dosen di tahun 2019. Ketertarikan bidang penelitiannya adalah elektronika industri, elektronika kontrol cerdas, elektronika daya, elektronika navigasi, *Internet of Things* (IoT), Energi Baru Terbarukan (EBT), sistem kelistrikan dan elektronika kapal. Dalam mewujudkan karir sebagai dosen profesional, penulis terus berupaya aktif dalam melakukan penelitian, pengabdian masyarakat, dan menulis baik dalam bentuk jurnal nasional maupun internasional.

BIODATA PENULIS



Muhammad Nuzan Rizki, S.T., M.T.

Dosen Program Studi Teknik Mesin
Fakultas Teknik Universitas Malikussaleh

Penulis lahir di Langsa tanggal 16 Januari 1998. Penulis adalah dosen tetap pada Program Studi Teknik Mesin Universitas Malikussaleh. Menyelesaikan pendidikan Sarjana Teknik Mesin dengan bidang Keahlian Konstruksi & Perancangan pada 2019 dan melanjutkan pendidikan Magister Teknik Mesin dengan bidang Keahlian Material & Manufaktur di Universitas Syiah Kuala pada 2020. Saat ini Penulis menekuni bidang penelitian mengenai pengaruh optimasi topologi desain terhadap sifat mekanik material. Penulis menaruh minat yang besar pada upaya merancang produk yang memiliki efisiensi bentuk mekanika paling optimal. Hasil penelitian ini bertujuan agar meningkatkan inovasi dalam konsep desain.

BIODATA PENULIS



Ir. Ali Impron, S.Kom., M.Kom.
Dosen Program Studi Informatika
Fakultas Teknik dan Pertanian
Universitas Muhammadiyah Sampit

Penulis lahir di Grobogan, Jawa Tengah, pada tahun 1983. Penulis adalah seorang dosen dan profesional IT dengan pengalaman lebih dari 17 tahun dalam mengelola layanan IT, internet service provider, dan industri pertambangan. Penulis memiliki keahlian dalam infrastruktur IT, IoT, Data Center, dan Business Intelligence. Saat ini, penulis menjabat sebagai Head of Information Technology di PT. Darma Henwa Tbk, di mana penulis bertanggung jawab untuk mengelola tim IT dan memastikan layanan IT berkualitas tinggi.

Penulis menyelesaikan gelar Sarjana Teknik Informatika dari STMIK AKAKOM Yogyakarta dan gelar Magister Teknologi Informasi dari Universitas Teknologi Digital Indonesia, Yogyakarta. Saat ini, penulis sedang menempuh Program Doktor Ilmu Teknik di Universitas Negeri Yogyakarta. Selain perannya di dunia industri, penulis juga tercatat sebagai dosen tetap di Universitas Muhammadiyah Sampit.

Selama karirnya, penulis telah memperoleh berbagai sertifikasi internasional yang mengakui keahliannya di bidang teknologi informasi, termasuk Microsoft Certified IT Professional (MCITP), Cisco Certified Network Associate (CCNA), dan Juniper Networks Certified Associate (JNCIA). Penulis memiliki minat besar dalam penelitian dan integrasi produk IT terbaru dengan proses bisnis, serta memiliki pemahaman mendalam tentang administrasi sistem, keamanan IT, dan jaringan.

BIODATA PENULIS



Tasrif Hasanuddin, S.T.,M.Cs

Dosen Program Studi Teknik Informatika
Fakultas Ilmu Komputer , Universitas Muslim Indonesia

Penulis lahir di Padang tanggal 10 Desember 1969. Penulis adalah dosen tetap pada Program Studi Teknik Informatika, Universitas Muslim Indonesia. Menyelesaikan pendidikan S1 pada Jurusan Teknik Elektro dan melanjutkan S2 pada Ilmu Komputer Universitas Gajah Mada.

BIODATA PENULIS



Yendi Putra, S. Kom., M. Kom, MTA

Dosen Program Studi Manajemen Informatika
Fakultas Ekonomi Universitas Mahaputra Muhammad Yamin

Penulis lahir di Salimpuang tanggal 03 Januari 1988. Penulis adalah dosen tetap pada Program Studi Manajemen Informatika Fakultas Ekonomi Universitas Mahaputra Muhammad Yamin. Pada tahun 2007 menyelesaikan pendidikan D1 di LKP Palapa Komputer Batusangkar dan melanjutkan Pendidikan S1 Jurusan Sistem Informasi tahun 2010 di STMIK Indonesia Padang selanjutnya menempuh Pendidikan Magister di Universitas Putra Indonesia (UPI YPTK-Padang) tahun 2018. Selain menjadi dosen penulis juga guru jurusan Rekayasa Perangkat Lunak pada SMK Maritim Nusantara dan juga menjadi Instruktur Komputer pada LPK Palapa Computer Batusangkar. Selain Akademisi Penulis juga seorang Praktisi bidang IT sebagai Ketua RTIK Wilayah Sumater Barat Periode 2025-2027, selain itu Penulis sangat tertarik pada bidang teknologi terutama bidang Internet of Things dan keamanan, pada saat studi S2 saya menulis tesis dengan menggunakan Algoritma Advance Encryption Standar untuk mengamankan Token sebuah website dari serangan Cros Site Script. Penulis sangat suka mengikuti lomba bidang komputer, pada tahun 2022 penulis mendapatkan

juara 3 pada ajang lomba Kompetensi Keterampilan Instruktur Nasional (KKIN) Wilayah Barat di Banda Aceh, Penulis memiliki 2 orang anak yang bernama ayumna usia 5 tahun dan Ibrahim usia 2 tahun.

BIODATA PENULIS



Frabowo Prasetia, S.Kom., M.T.I.

Dosen Program Studi Teknik Kimia Mineral
Politeknik ATI Makassar

Penulis lahir di Palopo tanggal 23 Agustus 1996. Penulis adalah dosen tetap pada Program Studi Teknik Kimia Mineral, Politeknik ATI Makassar. Menyelesaikan Pendidikan S1 pada Jurusan Teknik Informatika dan melanjutkan S2 pada Jurusan Megister Teknik Informatika. Penulis menekuni pada bidang Design Grafis dan menulis jurnal penelitian pada bidang Teknik Informatika.

Saat ini penulis sedang belajar melakukan penulisan terkait pada bidang Kimia Mineral namun pada bidang pemanfaatan teknologinya. Karya buku ini adalah pertama penulis buat sehingga dapat membantu penunjang karir kedepannya. Penulis dapat dihubungi di email *fprasetia@atim.ac.id*

BIODATA PENULIS



Dr. Fitri Puspasari, S.Si., M.Sc
Dosen Departemen Teknik Elektro dan Informatika
Sekolah Vokasi Universitas Gadjah Mada

Penulis adalah dosen tetap pada Departemen Teknik Elektro dan Informatika Sekolah Vokasi, Universitas Gadjah Mada. Penulis lahir di Sragen Tahun 1991 dan telah menyelesaikan pendidikan doktor di FMIPA UGM pada tahun 2024. Ia aktif terlibat dalam beberapa proyek penelitian dosen dan pengabdian kepada masyarakat yang bertujuan untuk mengembangkan dan mengimplementasikan keilmuannya.

BIODATA PENULIS



Muh. Agus, S.Kom., M.Kom.

Dosen Program Studi Ilmu Komputer
Institut Teknologi Bacharuddin Jusuf Habibie

Penulis lahir di Ugi Baru tanggal 21 Agustus 1995. Penulis adalah dosen tetap pada Program Studi Ilmu Komputer Jurusan Teknologi Produksi dan Industri Institut Teknologi Bacharuddin Jusuf Habibie. Menyelesaikan pendidikan S1 pada Program Studi Ilmu Komputer dan melanjutkan S2 pada Program Studi Ilmu Komputer. Penulis menekuni bidang Internet of Things.