

INTERNET OF THINGS: KONSEP DAN IMPLEMENTASINYA

**Purnawarman Musa
Amin Ama Duwila
Muhammad Irwan Syahib
Alex Copernikus Andaria
Yendi Putra
Kusnaeni
Hamdan Gani
Muhammad Fadli Azis
Asma Ainuddin
Julianti Habibuddin
Muhammad Sainal Abidin
Tino Suhaebri**



GET PRESS INDONESIA

INTERNET OF THINGS: KONSEP DAN IMPLEMENTASINYA

Penulis :

Purnawarman Musa
Amin Ama Duwila
Muhammad Irwan Syahib
Alex Copernikus Andaria
Yendi Putra
Kusnaeni
Hamdan Gani
Muhammad Fadli Azis
Asma Ainuddin
Julianti Habibuddin
Muhammad Sainal Abidin
Tino Suhaebri

ISBN :

Editor : Tri Putri Wahyuni., S.Pd

Penyunting : Diana Purnama Sari., SE.M.E

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

Penerbit : GET PRESS INDONESIA

Anggota IKAPI No. 033/SBA/2022

Redaksi :

Jln. Palarik Air Pacah No 26 Kel. Air Pacah
Kec. Koto Tangah Kota Padang Sumatera Barat
Website : www.getpress.co.id
Email : adm.getpress@gmail.com

Cetakan pertama, Juni 2024

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

KATA PENGANTAR

Segala Puji dan syukur atas kehadiran Allah SWT dalam segala kesempatan. Sholawat beriring salam dan doa kita sampaikan kepada Nabi Muhammad SAW. Alhamdulillah atas Rahmat dan Karunia-Nya penulis telah menyelesaikan Buku *Internet Of Things: Konsep Dan Implementasinya* ini.

Buku Ini Membahas Pengenalan *Internet Of Things* (IoT), Arsitektur IoT, Protokol Komunikasi Dalam IoT, Sensor Dan Aktuator Pada IoT, Keamanan Dan Privasi Dalam IoT, Penanganan Big Data Pada IoT, Pemanfaatan Machine Learning Dalam IoT, Implementasi IoT Pada Smart Home, Implementasi IoT Pada Smart City, Implementasi IoT Pada Pertanian, Implementasi IoT Pada Kesehatan, Implementasi IoT Pada Lingkungan Hidup.

Proses penulisan buku ini berhasil diselesaikan atas kerjasama tim penulis. Demi kualitas yang lebih baik dan kepuasan para pembaca, saran dan masukan yang membangun dari pembaca sangat kami harapkan.

Penulis ucapkan terima kasih kepada semua pihak yang telah mendukung dalam penyelesaian buku ini. Terutama pihak yang telah membantu terbitnya buku ini dan telah mempercayakan mendorong, dan menginisiasi terbitnya buku ini. Semoga buku ini dapat bermanfaat bagi masyarakat Indonesia.

Padang, Juni 2024

Penulis

DAFTAR ISI

KATA PENGANTAR	i
DAFTAR ISI	ii
DAFTAR GAMBAR	viii
DAFTAR TABEL	xi
BAB 1 PENGENALAN INTERNET OF THINGS (IOT)	1
1.1 Pendahuluan.....	1
1.2 Prinsip Kerja <i>Internet of Things</i> (IoT)	2
1.3 Definisi IoT.....	3
1.3.1 Perkembangan IoT	4
1.3.2 Sejarah Prinsip Kerja IoT.....	4
1.3.3 Proses Kerja Dasar pada IoT	6
1.4 Penerapan dan Manfaat IoT	7
1.4.1 Smart Home	9
1.4.2 Industri dan Manufaktur	9
1.4.3 Kesehatan dan Perawatan Kesehatan	9
1.5 Tantangan dan Etika.....	9
1.5.1 Keamanan dan Privasi	10
1.5.2 Standardisasi.....	10
1.5.3 Kapasitas dan Keterbatasan Energi	10
1.5.4 Integrasi dan Keterhubungan.....	10
1.5.5 Biaya Implementasi.....	10
1.5.6 Isu Hukum dan Etika	11
1.5.7 Skala dan Kebutuhan Bandwidth.....	11
1.6 Kesimpulan	11
DAFTAR PUSTAKA	12
BAB 2 ARSITEKTUR IoT	15
2.1 Pendahuluan.....	15
2.2 Komponen Utama Arsitektur IoT.....	17
2.2.1 Sensor dan Aktuator	17
2.2.2 Media Komunikasi Digital untuk IoT.....	17
2.3 Lapisan Arsitektur IoT	21
2.3.1 Arsitektur 3 Lapis	21
2.3.2 Arsitektur 5 Lapis	22
2.3.3 Arsitektur 7 Lapis	24
2.4 Arsitektur Referensi IoT	27

2.4.1 Model Referensi IoT - ITU.....	27
2.4.2 Model Referensi IoT - CISCO	28
2.5 Persyaratan untuk Arsitektur IoT	31
2.5.1 Kontrol Sumber Daya.....	31
2.5.2 Kesadaran Energi	31
2.5.3 Kualitas Layanan	31
2.5.4 Interoperabilitas	32
2.5.5 Manajemen interferensi	32
2.5.6 Keamanan.....	32
DAFTAR PUSTAKA.....	34
BAB 3 PROTOKOL KOMUNIKASI DALAM IOT	37
3.1 Pendahuluan	37
3.2 Jenis-jenis Protokol Komunikasi IoT.....	37
3.2.1 Message Queuing Telemetry Transport.....	37
3.2.2 Advanced Message Queuing Protocol	39
3.2.3 Extensible Messaging and Presence Protocol.....	41
3.2.4 <i>Lightweight Machine to Machine</i>	42
3.2.5 Bluetooth.....	44
3.2.6 <i>Zigbee</i>	45
3.2.7 LoRa dan LoRaWAN	47
DAFTAR PUSTAKA.....	49
BAB 4 SENSOR DAN AKTUATOR PADA IOT	51
4.1 Pendahuluan	51
4.2 Sensor dalam IoT	52
4.2.1 Jenis dan Fungsi Sensor pada IoT	52
4.2.2 Karakteristik Sensor Suhu pada IoT.....	54
4.2.3 Desain dan Konfigurasi Sistem Sensor pada IoT...	57
4.3 Aktuator dalam IoT	57
4.3.1 Prinsip Kerja Aktuator pada IoT.....	58
4.3.2 Jenis-Jenis penguatan Aktuator pada IoT	58
4.3.3 Desain dan Konfigurasi Sistem Aktuator pada IoT	63
DAFTAR PUSTAKA.....	64
BAB 5 KEAMANAN DAN PRIVASI DALAM IOT	67
5.1 Pendahuluan	67
5.2 Definisi Keamanan dan Privasi dalam IoT.....	68
5.3 Pentingnya Keamanan dan Privasi dalam IoT	69

5.4 Jenis Kasus Serangan Pada IOT	70
5.5 Ancaman Keamanan dalam IoT	79
5.5.1 Eksploitasi Kerentanan Perangkat Lunak dan Perangkat Keras	79
5.5.2 Serangan Melalui Jaringan.....	79
5.5.3 Serangan Fisik.....	80
5.6 Privasi dalam IoT	80
5.6.1 Risiko Privasi dalam Penggunaan IoT	81
5.6.2 Data Sensitif dalam IoT.....	84
5.6.3 Pengumpulan dan Pengolahan Data	85
5.6.4 Privasi Pengguna dan Kepatuhan Regulasi	86
5.7 Teknologi Keamanan Untuk IoT	87
5.7.1 Enkripsi dan Keamanan Data	87
5.7.2 Perlindungan Data	92
5.7.3 Penggunaan Kunci.....	92
5.7.4 Implementasi pada IoT.....	92
5.8 Autentikasi dan Otorisasi.....	93
5.8.1 Autentikasi.....	93
5.8.1 Otorisasi	94
5.9 Keamanan Jaringan dan Komunikasi.....	95
5.9.1 Keamanan Jaringan	95
5.9.2 Keamanan Komunikasi	95
5.9.3 Penggunaan Protokol Keamanan.....	96
5.9.4 Pemantauan dan Pembaruan	96
5.9.5 Strategi dan Praktik Keamanan dalam IoT	97
5.9.6 Mengidentifikasi dan Mengelola Risiko pada IoT.....	97
5.9.7 Pembaruan dan Manajemen Perangkat.....	98
5.9.8 Framwork Keamanan IOT	98
5.10 Regulasi dan Standar Keamanan IoT	102
5.10.1 Regulasi Global.....	102
5.10.2 Regulasi Lokal	102
5.11 Dampak Regulasi pada Pengembangan dan Implementasi IoT	103
5.12 Masa Depan Keamanan dan Privasi dalam IoT	104
5.12.1 Tren dan Inovasi Teknologi Keamanan IoT	104
5.12.3 Tantangan dan Peluang di Masa Depan IOT	105
DAFTAR PUSTAKA	108

BAB 6 PENANGANAN BIG DATA PADA INTERNET OF THINGS (IOT)	111
6.1 Pengertian Big Data	111
6.2 Karakteristik Big Data	111
6.2.1 <i>Volume</i>	112
6.2.2 <i>Velocity</i>	113
6.2.3 <i>Variety</i>	114
6.2.4 <i>Veracity</i>	114
6.2.5 <i>Value</i>	115
6.3 Teknologi Pendukung Big Data	116
6.3.1 Infrastruktur Penyimpanan	117
6.3.2 Pemrosesan Data	117
6.3.3 Analisis Data	119
DAFTAR PUSTAKA	122
BAB 7 PEMANFAATAN MACHINE LEARNING DALAM IOT	123
7.1 Pendahuluan	123
7.1.1 Definisi dan Konsep Dasar <i>Machine Learning</i> (ML)	123
7.1.2 Definisi dan Konsep Dasar <i>Internet of Things</i> (IoT)	124
7.2 Integrasi ML dalam Ekosistem IoT	126
7.2.1 Keuntungan penggunaan ML dalam analisis data IoT	126
7.2.2 Peningkatan efisiensi melalui ML dalam pengambilan keputusan	128
7.3 Contoh Kasus Penggunaan ML dalam IoT	130
7.3.1 Prediksi dan analisis data sensor	130
7.3.2 Deteksi anomali dan keamanan IoT	131
7.4 Tantangan dan Hambatan dalam Pemanfaatan ML dalam IoT	133
7.4.1 Skala dan Volume Data	133
7.4.3 Keamanan dan Privasi	137
7.5 Peluang dan Tren Masa Depan	139
7.6 Kesimpulan	141
DAFTAR PUSTAKA	143

BAB 8 IMPLEMENTASI IOT PADA SMART HOME.....	147
8.1 Konsep Smart Home	147
8.2 Implementasi IoT pada Smart Home	148
8.3 Contoh Implementasi IoT pada Smart Home.....	149
8.3.1 Smart Light.....	149
8.3.2 Smart Plug.....	150
8.3.3 Smart Door Lock.....	150
8.3.4 Smart Security Camera.....	151
8.3.5 Smart Appliances	152
8.3.6 Smart Pet Feeder.....	152
8.3.7 Smart Speaker	153
8.4 Platform IoT Smart Home.....	154
8.4.1 Bardi Smart Home.....	155
8.4.2 Samsung SmartThings	155
8.4.3 Xiaomi Smart Home	155
8.4.4 Google Home	156
8.4.5 Apple HomeKit.....	156
8.4.6 Amazon Alexa	156
DAFTAR PUSTAKA	157
BAB 9 IMPLEMENTASI IOT PADA SMART CITY	159
9.1 Smart City	159
9.2 Konsep SMART City.....	160
9.3 Penerapan Smart City Pada Kota Besar Di Indonesia..	162
9.3.1 Jakarta	162
9.3.2 Surabaya	163
9.3.3 Yogyakarta.....	164
9.3.4 Makassar.....	166
9.4 Smart City berbasis IoT	167
9.4.1 Smart Traffic Light	168
9.4.2 Smart Grid.....	170
DAFTAR PUSTAKA	172
BAB 10 IMPLEMENTASI IOT PADA PERTANIAN	
RUMAH JAMUR	175
10.1 Pendahuluan.....	175
10.1.1 Pengertian <i>IoT</i>	175
10.1.2 Rumah Jamur	176
10.2 Prinsip Kerja <i>IoT</i> pada Rumah Jamur.....	177

10.3 Penerapan <i>IoT</i> pada Rumah Jamur	178
10.3.1 Monitoring Suhu dan Kelembapan	179
10.3.2 Penyiraman Otomatis	183
DAFTAR PUSTAKA	185
BAB 11 IMPLEMENTASI IOT PADA KESEHATAN.....	187
11.1 Pendahuluan	187
11.2 Pemantauan kesehatan.....	188
11.3 Telemedicine.....	194
11.4 Rekam Medis.....	195
DAFTAR PUSTAKA.....	198
BAB 12 IOT DALAM BIDANG LINGKUNGAN	201
12.1 Ruang Lingkup.....	201
12.2 <i>Smart Environment Monitoring (SEM)</i>	206
12.3 Sensor Pendeteksi Kondisi Lingkungan.....	208
12.4 Sensor Kualitas Udara.....	209
12.5 Sensor Kualitas Air	212
12.6 Pemantauan Kualitas Udara dan Air Berbasis ESP32	215
DAFTAR PUSTAKA.....	218
BIODATA PENULIS	

DAFTAR GAMBAR

Gambar 1.1. Perkembangan IoT dari waktu ke waktu	3
Gambar 1.2. Perkembangan IoT dari waktu ke waktu	6
Gambar 1.3. Progres dan Keunggulan <i>Internet of Things</i> (IoT).....	9
Gambar 2.1. IoT technology architecture	15
Gambar 2.2. <i>Infrastructure and functional component for the Internet of Things</i>	20
Gambar 2.3. Arsitektur IoT - 3 Lapis	22
Gambar 2.4. Arsitektur IoT – 5 Lapis.....	23
Gambar 2.5. Komponen Pendekatan 4 Tahap	25
Gambar 2.6. Arsitektur IoT empat tahap untuk data yang sangat besar	27
Gambar 2.7. ITU – IoT Reference Model.....	28
Gambar 2.8. CISCO – IoT Reference Model	29
Gambar 2.9. Persyaratan Utama Arsitektur IoT Masa Depan	33
Gambar 3.1. Protokol MQTT	38
Gambar 3.2. Protokol AMQP	40
Gambar 3.3. Protokol XMPP	41
Gambar 3.4. Protokol LwM2M	42
Gambar 3.5. Arsitektur Zigbee	46
Gambar 3.6. Arsitektur LoRa dan LoRaWAN	47
Gambar 4.1. Contoh Sensor Dalam Perangkat IoT	51
Gambar 4.2. LM35 Jangkauan Penuh	55
Gambar 4.3. Pinout Modul Sensor DHT11 dan DHT22	56
Gambar 4.4. Pinout Modul Sensor DS18B20	57
Gambar 4.5. Motor servo.....	59
Gambar 4.6. Motor stepper	60
Gambar 4.7. Motor DC.....	60
Gambar 4.8. Aktuator Piston Pneumatik	61
Gambar 5.1. Ilustrasi IOT	81
Gambar 5.2. Proses Enkripsi Asymmetric.....	88
Gambar 5.3. Algoritma AES.....	89
Gambar 5.4. Autentikasi pada IoT.....	93
Gambar 5.5. Standar Keamanan ISO/IEC 27001	103

Gambar 6.1. Karakteristik Big Data	111
Gambar 6.2. Tools Big Data	116
Gambar 7.1. Supervised Learning.....	124
Gambar 7.2. Integrasi IoT dan ML	128
Gambar 8.1. Perangkat pintar pada Smart Home	148
Gambar 8.2. Smart Light.....	149
Gambar 8.3. Smart Plug	150
Gambar 8.4. Smart Door Lock.....	151
Gambar 8.5. Smart security camera	151
Gambar 8.6. Smart Appliances	152
Gambar 8.7. Smart Pet Feeder.....	153
Gambar 8.8. Smart Speaker	154
Gambar 8.9. Platform IoT Smart Home	155
Gambar 9.1. Konsep Smart City	161
Gambar 9.2. Komponen smart city	168
Gambar 9.3. Desain system smart traffic light.....	169
Gambar 9.4. Konsep smart grid	170
Gambar 10.1. Rangkaian Monitoring Temperatur dan Kelembapan	180
Gambar 10.2. Coding diagram json monitoring temperatur dan kelembapan.....	183
Gambar 11.1. Pasien Monitor	189
Gambar 11.2. Pulse Oxymetri	189
Gambar 11.3. Max30100	190
Gambar 11.4. Wemos R1 mini Esp8266.....	190
Gambar 11.5. Blok diagram pulse Oxymetri berbasis IoT.....	191
Gambar 11.6. Alat pulse Oxymetri berbasis IoT	191
Gambar 11.7. Tampilan Hasil Pengukuran Pada Smartphone	192
Gambar 11.8. Infus Pump.....	193
Gambar 11.9. Monitoring unfus berbasis IoT.....	193
Gambar 11.10. Aplikasi Halodoc.....	195
Gambar 11.11. Topologi Rekam Medis Berbasis IoT.....	196
Gambar 11.12. Rekam Medis Dengan Sidik Jari.....	197
Gambar 12.1. Arsitektur IoT pada Lingkungan Cerdas	202
Gambar 12.2. Lingkungan Cerdas	205

Gambar 12.3. Penerapan SEM.....	207
Gambar 12.3. Rangkaian Sensor (a) tipe MQ-x dan (b) TGS-x	211
Gambar 12.4. Sensor Thermistor NTC 3950.....	213
Gambar 12.5. Sensor Thermistor NTC 3950.....	214
Gambar 12.6. Sensor PH.....	215
Gambar 12.7. Diagram Sistem Pemantauan Lingkungan Berbasis IoT.....	217

DAFTAR TABEL

Tabel 2.1. Lapisan pada Arsitektur IoT	24
Tabel 4.1. Jenis-Jenis Sensor pada IoT berdasarkan fungsi	52
Tabel 4.2. Perbandingan Karakteristik Modul DHT11 dan DHT22	55
Tabel 5.1. Jenis Serangan Pada IoT.....	70
Tabel 12.1. Sensor Gas dan Kualitas Udara	210

BAB 1

Pengenalan Internet of Things (IoT)

Oleh Purnawarman Musa

1.1 Pendahuluan

Sebagai pengantar, bab ini akan memberikan pemahaman lebih mendalam dan esensi *Internet of Things* (IoT) dengan merinci konsep dasarnya. Pembahasan yang terkait definisi IoT hingga perkembangan sejarahnya, serta akan menjelajahi prinsip kerja yang mendasari teknologi ini. Selanjutnya, dalam bab ini akan membahas beragam penerapan nyata dan manfaat yang telah dihadirkan oleh kehadiran IoT dalam kehidupan sehari-hari pengguna sehingga dapat memahami bagaimana IoT menjadi suatu perangkat yang dapat mempercepat perubahan secara signifikan dalam tata cara hidup dan berinteraksi di era digital ini.

Pada tahun 2005, *International Telecommunications Union* (ITU) menerbitkan laporan pertamanya tentang *Internet of Things* (IoT), mencatat bahwa "Komunikasi mesin ke mesin dan komunikasi orang ke komputer akan diperluas ke perangkat, mulai dari objek rumah tangga sehari-hari hingga sensor yang memantau gerakan Jembatan Golden Gate atau mendeteksi gempa bumi. Semuanya, mulai dari ban hingga sikat gigi, akan berada dalam jangkauan komunikasi, membawa kabar datangnya era baru, di mana internet saat ini (data dan orang) akan memberikan jalan bagi *Internet of Things* pada masa mendatang." (Benomar et al., 2021).

Internet of Things (IoT) tidak hanya menjadi trend teknologi, melainkan suatu pergeseran paradigma dalam cara pengunanya memandang dan mengintegrasikan perangkat dalam kehidupan sehari-hari (Madakam et al., 2015). Sejak diperkenalkan pertama kali konsep IoT, telah terjadi perubahan yang merubahkan dan memainkan peran sentral dalam mendefinisikan cara pengunanya bekerja, tinggal, dan bermain. Mengapa IoT telah menjadi suatu

kebutuhan yang penting dalam keseharian, beberapa hasil penelitian terkait teknologi IoT diantaranya (J. Showail, 2021; Pedro García Márquez, 2021; Sethi & Sarangi, 2017);

1. Konektivitas yang Tanpa Batas

IoT memungkinkan perangkat untuk berkomunikasi melalui jaringan, menciptakan suatu lingkungan yang serba terhubung. Mulai dari perangkat rumah tangga hingga kendaraan dan infrastruktur kota, semua dapat bersinergi untuk memberikan pengalaman yang lebih baik dan efisien.

2. Optimasi dan Efisiensi

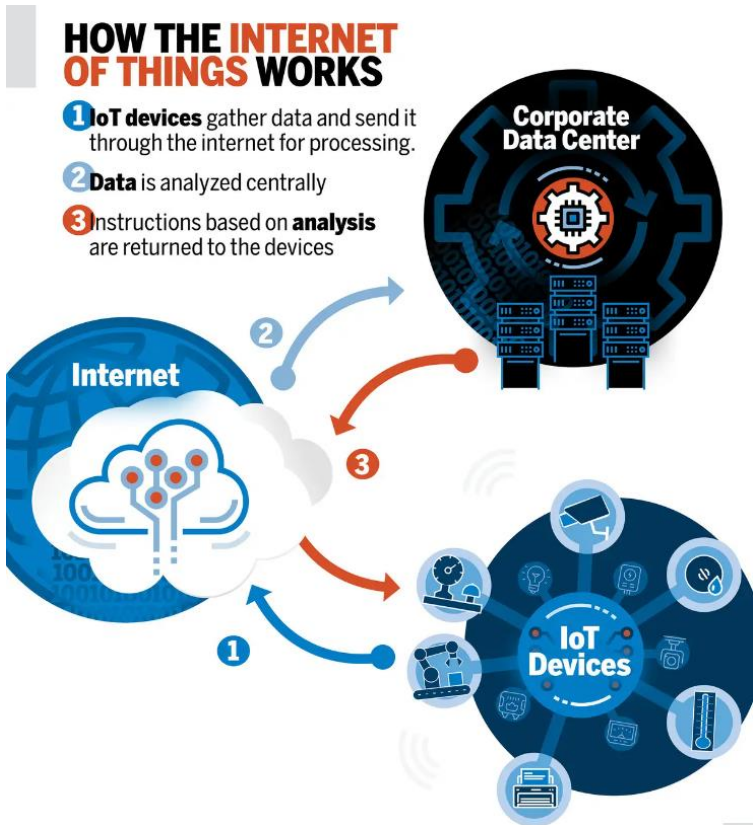
Dengan sensor yang terus menerus mengumpulkan data, IoT memungkinkan pengoptimalan proses dan pengambilan keputusan berdasarkan informasi real-time. Proses optimalisasi dan efisiensi bukan saja menaikkan efisiensi operasional, namun mengarah pada penggunaan sumber daya yang lebih cerdas.

3. Inovasi dalam Beberapa Bidang Pekerjaan

Penerapan IoT sudah merambah di beberapa bidang, termasuk manufaktur, kesehatan, pertanian, dan banyak lagi. Inovasi ini menciptakan peluang baru, merangsang pertumbuhan ekonomi, dan membuka pintu bagi solusi-solusi yang lebih pintar.

1.2 Prinsip Kerja *Internet of Things* (IoT)

Pemahaman yang mendalam tentang prinsip kerja IoT, bertujuan untuk menggali potensi besar yang dimiliki oleh Internet of Things dalam meningkatkan efisiensi, kenyamanan, dan inovasi di berbagai sektor kehidupan (Ebling, 2016).



Gambar1.1. Perkembangan IoT dari waktu ke waktu
(Sumber: (Fruhlinger, 2022))

1.3 Definisi IoT

Internet of Things (IoT) merujuk pada suatu konsep di mana perangkat fisik, objek, atau sistem memiliki kemampuan untuk saling berkomunikasi dan bertukar data melalui jaringan internet tanpa intervensi manusia (Kumar, 2021). Prinsip utama dari IoT adalah memberdayakan perangkat yang telah ditanamkan suatu sistem untuk mengumpulkan, mentransmisikan, dan merespons data secara otomatis, menciptakan lingkungan yang lebih terhubung dan cerdas.

1.3.1 Perkembangan IoT

Perkembangan IoT telah melalui evolusi yang signifikan, dimana fokus utama adalah pada konektivitas antarperangkat. Namun, seiring dengan kemajuan teknologi sensor, pengembangan protokol komunikasi yang efisien, dan peningkatan kapabilitas komputasi, IoT telah berkembang menjadi ekosistem yang mendukung aplikasi yang lebih kompleks (International Telecommunication Union, 2012; Youssef & Hassan, 2019). Perkembangan ini mencakup penggunaan sensor yang lebih canggih, peningkatan keamanan, dan integrasi dengan teknologi lain seperti *Big Data*, kecerdasan buatan (AI) dan komputasi awan.

1.3.2 Sejarah Prinsip Kerja IoT

Perkembangan Internet of Things melalui serangkaian inovasi dan evolusi teknologi dengan konsep konektivitas tanpa batas. Kemajuan dalam sensor, komputasi, dan konektivitas nirkabel telah menjadi pendorong utama dalam pengembangan IoT.

Awal Mula Konsep IoT (2000-an)

Sejarah Internet of Things (IoT) dimulai pada awal tahun 2000-an ketika konsep konektivitas antarperangkat pertama kali muncul. Ide dasarnya adalah menghubungkan objek-objek fisik ke internet, memungkinkan mereka berkomunikasi dan bertukar data tanpa intervensi manusia. Pada periode ini, teknologi identifikasi frekuensi radio (RFID) dan sensor sederhana menjadi pionir dan sensor-sensor sederhana menjadi fondasi untuk menghubungkan objek secara langsung ke internet.

Perkembangan Sensor dan Komunikasi (2010-an)

Pada dekade 2010-an, perkembangan teknologi sensor dan protokol komunikasi menjadi pendorong utama pertumbuhan IoT. Sensor-sensor yang semakin canggih dan teknologi komunikasi yang lebih handal memungkinkan perangkat untuk mengumpulkan data dengan akurasi tinggi, perangkat untuk mengirimkan dan menerima data dengan lebih cepat dan efisien.

Menurut (Park & Nam, 2020), protokol komunikasi seperti MQTT (*Message Queuing Telemetry Transport*) dan CoAP

(*Constrained Application Protocol*) memberikan cara efisien untuk mentransmisikan data melalui jaringan yang digunakan secara luas.

Pertumbuhan Jaringan dan Konektivitas (2010-an)

Perkembangan infrastruktur jaringan dan konektivitas nirkabel menjadi langkah penting dalam sejarah IoT. Peningkatan kecepatan internet, pengembangan jaringan 4G, dan 5G membuka pintu bagi perangkat IoT untuk berkomunikasi secara lebih cepat dan efisien. Konektivitas yang semakin handal inilah yang memungkinkan pertumbuhan ekosistem IoT di berbagai sektor.

Integrasi dengan Teknologi Lain (2010-an hingga Sekarang)

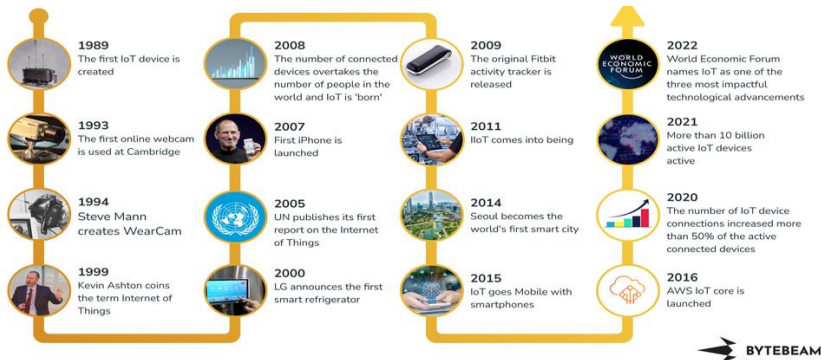
Peningkatan kapabilitas komputasi dan pertumbuhan teknologi terkait seperti kecerdasan buatan (AI) telah membantu meningkatkan kemampuan analisis data IoT. Ini membuka pintu bagi pengambilan keputusan yang lebih cerdas dan aksi otomatis yang lebih kompleks dan prediksi yang lebih akurat. Selain itu, komputasi awan juga berperan penting dalam menyimpan dan memproses volume besar data IoT.

Penerapan di Berbagai Sektor (2010-an hingga Sekarang)

Penerapan IoT tidak terbatas pada satu sektor tertentu. Dalam sejarahnya, IoT telah merambah ke berbagai bidang, termasuk manufaktur, pertanian, kesehatan, transportasi, dan rumah pintar. Penggunaan sensor dan perangkat pintar telah mengubah cara operasi dan pengelolaan di berbagai industri, meningkatkan efisiensi dan produktivitas.

Tantangan dan Keamanan (2010-an hingga Sekarang)

Seiring dengan pertumbuhan positif, IoT juga dihadapkan pada sejumlah tantangan. Salah satunya adalah keamanan. Karena banyaknya perangkat yang terhubung, keamanan data dan privasi menjadi fokus utama untuk menjaga keandalan dan adopsi luas teknologi ini.



Gambar1.2. Perkembangan IoT dari waktu ke waktu
(Sumber: (Kulkarni, 2022))

Sejarah *Internet of Things* mencerminkan perjalanan panjang dari konsep sederhana hingga menjadi perangkat yang integral secara transformasi digital. Dengan terus berkembangnya teknologi, IoT terus menjadi pendorong inovasi, membawa perubahan signifikan dalam cara manusia akan berinteraksi dengan dunia secara teknologi digital di kehidupan sehari-hari.

1.3.3 Proses Kerja Dasar pada IoT

Proses kerja dasar IoT terdapat 4 (empat) langkah utama:

1. Pengumpulan Data: Sensor dan perangkat pemantauan secara pintar mengumpulkan data dari lingkungan sekitarnya (Ariffudin & Musa, 2022). Oleh karena itu, IoT perlu didukung oleh sensor dan perangkat pintar yang difungsikan untuk mendapatkan suatu informasi seperti mendeteksi, mengukur, dan mengumpulkan data dari lingkungan sekitar. Contohnya termasuk sensor suhu (Dan et al., 2015; Musa et al., 2019), kelembaban (Zou et al., 2017), gerakan (Gozali et al., 2017), dan banyak lagi. Perangkat yang selanjutnya objek akan bertindak sebagai mata dan telinga yang terus-menerus dengan cara mengamati dan mendengarkan lingkungan yang berada di sekitarnya (Wilianto & Kurniawan, 2018).
2. Koneksi dan Komunikasi: Kunci utama dari IoT adalah kemampuan perangkat untuk terhubung satu sama lain melalui jaringan seperti membutuhkan koneksi jaringan

internet. Proses data didapat dari suatu perangkat akan dikirimkan melalui jaringan internet menggunakan protokol komunikasi khusus, seperti MQTT. Tujuan data dikirimkan agar memberikan informasi, disimpan dan dikumpulkan pada penyimpanan data, dan dapat dianalisa untuk mendapatkan suatu hasil keputusan tertentu sehingga memungkinkan perangkat untuk saling berbagi informasi secara efisien dan aman.

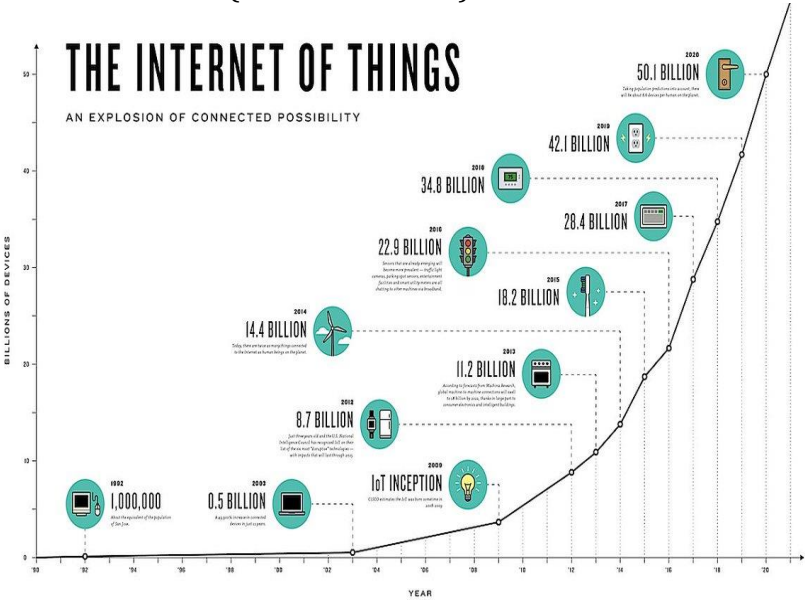
3. **Pengolahan Data:** Data yang dikumpulkan oleh perangkat IoT tidak hanya berguna jika disimpan secara mentah. Proses pengolahan data menjadi informasi yang bermakna terjadi di perangkat atau di cloud, memungkinkan pengambilan keputusan yang lebih cerdas (Asman et al., 2019). Apabila membutuhkan hasil yang memiliki kemampuan dalam pengambilan keputusan yang cerdas, maka data akan diolah menggunakan teknologi kecerdasan buatan.
4. **Aksi Otomatis:** Salah satu kekuatan utama IoT adalah kemampuannya untuk merespons secara otomatis terhadap informasi yang diterimanya. Ini dapat mencakup pengaturan perangkat, pengiriman notifikasi, atau bahkan tindakan fisik berdasarkan pada kondisi tertentu. Berdasarkan data atau informasi tersebut melalui pengolahan data, maka perangkat dapat mengambil tindakan otomatis atau memberikan notifikasi.

1.4 Penerapan dan Manfaat IoT

Di era awal tahun 2000-an, integrasi komputer dan gawai (perangkat mobile) memunculkan inovasi perangkat seperti handphone, menjadi salah satu perangkat paling dibutuhkan saat ini. Diperkirakan bahwa hampir sekitar seratusan miliar alat yang dihubungkan ditahun 2020, di mana kurang lebih 50 miliar di antaranya dengan memanfaatkan Internet of Things (IoT).

Selain itu, sejak 2018, IoT diproyeksikan untuk mencapai jumlah handphone, termasuk kendaraan bergerak, peralatan listrik, wearable, dan perangkat lainnya dengan saling dihubungkan. Perkembangan IoT sejak 2016 hingga 2022, diprediksi bahwa

jumlah peralatan yang memiliki teknologi IoT akan naik hingga mencapai 21%, hal ini disupor oleh perkembangan dan adopsi teknologi kebaruan. Selain itu, diakhir 2016, tercatat bahwa 400 juta perangkat berbasis IoT dapat terhubung dengan handphone, dan sehingga mencapai hasilnya diperkirakan akan mencapai 1,5 miliar peralatan berteknologi IoT ditahun 2022, atau dengan kata lain hasil pencapaian kurang lebih sebesar 70% dari kategori jaringan wide-area network. Hasil (lihat **Gambar1.3**).



Gambar1.3. Progres dan Keunggulan Internet of Things (IoT)
(Sumber: (Gudnyus.id, 2019))

Dalam keseharian, cara pengguna melihat implementasi IoT di berbagai sektor. Rumah pintar memanfaatkan IoT untuk mengontrol pencahayaan, suhu, dan keamanan, sementara industri menggabungkan IoT untuk menciptakan lingkungan manufaktur yang lebih adaptif dan efisien. Bahkan, sektor kesehatan merasakan dampak positif melalui penggunaan perangkat medis terhubung yang memberikan pemantauan pasien yang lebih baik.

1.4.1 Smart Home

Salah satu contoh penerapan yang paling umum dari IoT adalah di lingkungan rumah pintar. Dengan menggunakan perangkat seperti lampu pintar, termostat pintar, dan kamera keamanan yang terhubung, pengguna dapat mengontrol dan memantau rumah mereka dari jarak jauh.

1.4.2 Industri dan Manufaktur

Dalam industri, IoT digunakan untuk menciptakan lingkungan manufaktur yang lebih cerdas. Sensor pada peralatan mesin dapat memberikan data real-time tentang kinerja dan kondisi, memungkinkan perawatan yang tepat waktu dan efisiensi operasional yang lebih tinggi.

1.4.3 Kesehatan dan Perawatan Kesehatan

Di bidang kesehatan, IoT memungkinkan monitoring pasien secara real-time melalui perangkat medis yang terhubung. Ini tidak hanya meningkatkan pengawasan, tetapi juga memungkinkan pelayanan kesehatan untuk memberikan perawatan yang lebih personal dan efisien.

1.5 Tantangan dan Etika

Seiring dengan segala inovasi, IoT juga dihadapkan pada tantangan. Keamanan data dan privasi menjadi fokus utama, sementara isu-isu etika terkait dengan pengumpulan dan penggunaan data memerlukan perhatian serius (Khan & Salah, 2018; Lee & Lee, 2015). Penting bagi pengguna untuk mendalami, memahami dan mengatasi tantangan ini guna memastikan bahwa kemajuan teknologi menciptakan dampak positif.

Penerapan *Internet of Things* (IoT) membawa dampak positif yang signifikan, tetapi tidak terlepas dari sejumlah tantangan yang perlu diatasi untuk memastikan keberlanjutan dan keberhasilan teknologi ini. Pada sub-bagian ini, terdapat beberapa tantangan utama yang dihadapi dalam pemanfaatan IoT.

1.5.1 Keamanan dan Privasi

Tantangan terbesar dalam penerapan IoT adalah keamanan data. Dengan semakin banyaknya perangkat yang terhubung, risiko terjadinya pelanggaran keamanan meningkat. Keamanan perangkat, enkripsi data, dan manajemen akses yang tidak memadai dapat membuka celah bagi potensi ancaman keamanan. Selain itu, perlindungan privasi pengguna menjadi isu sentral, terutama dalam pengumpulan dan analisis data yang besar.

1.5.2 Standardisasi

Kekurangan standar yang konsisten menjadi tantangan dalam ekosistem IoT. Perbedaan dalam protokol komunikasi, format data, dan interoperabilitas antarperangkat dapat menghambat integrasi yang efektif. Standarisasi yang lebih baik diperlukan untuk memastikan bahwa perangkat dari berbagai produsen dapat berkomunikasi dan bekerja bersama tanpa hambatan.

1.5.3 Kapasitas dan Keterbatasan Energi

Banyak perangkat IoT beroperasi dengan daya yang terbatas. Keterbatasan kapasitas baterai atau sumber daya lainnya pada perangkat dapat menjadi hambatan untuk pengiriman data yang konsisten. Meningkatkan efisiensi energi dan pengembangan teknologi baterai yang lebih baik menjadi perhatian penting.

1.5.4 Integrasi dan Keterhubungan

Integrasi IoT dengan infrastruktur yang ada seringkali rumit. Banyak organisasi memiliki sistem legacy yang sulit diintegrasikan dengan solusi IoT baru. Selain itu, menciptakan lingkungan terhubung yang konsisten dan saling terkait memerlukan upaya dan investasi yang signifikan.

1.5.5 Biaya Implementasi

Biaya awal implementasi teknologi IoT, termasuk perangkat keras, perangkat lunak, dan pelatihan, dapat menjadi hambatan utama, terutama bagi organisasi kecil dan menengah. Meskipun seiring waktu biaya ini dapat turun, tetapi masih menjadi

pertimbangan utama dalam pengambilan keputusan untuk mengadopsi teknologi IoT.

1.5.6 Isu Hukum dan Etika

Pengumpulan dan penggunaan data oleh perangkat IoT menghadapi tantangan hukum dan etika. Pertanyaan mengenai kepemilikan data, hak privasi, dan tanggung jawab dalam penggunaan data perlu diatasi. Kekhawatiran masyarakat terhadap penyalahgunaan data menjadi isu utama yang harus diakui dan ditangani.

1.5.7 Skala dan Kebutuhan Bandwidth

Dengan pertumbuhan jumlah perangkat IoT, dibutuhkan kapasitas jaringan yang lebih besar. Keterbatasan bandwidth dapat menjadi hambatan dalam mentransmisikan volume besar data secara efisien, terutama dalam skenario di mana banyak perangkat harus berkomunikasi secara bersamaan.

1.6 Kesimpulan

Pengenalan *Internet of Things* (IoT) mencerminkan perjalanan melalui era digital yang menakjubkan. Dari konsep awal hingga implementasi di berbagai sektor kehidupan, IoT telah menjadi kekuatan pendorong revolusi digital. *Internet of Things* (IoT) tidak hanya merupakan suatu teknologi tambahan, melainkan merupakan pilar utama dalam revolusi digital. Konsep IoT telah mengubah paradigma konvensional tentang bagaimana perangkat dan objek dapat saling berinteraksi, menciptakan suatu ekosistem yang membawa dampak transformasional pada berbagai aspek kehidupan. Pada dasarnya, IoT dapat dikatakan sebagai perangkat inovasi yang menciptakan jaringan tak terlihat di sekitar lingkungan pengguna, di mana perangkat, kendaraan, dan objek lainnya dapat terhubung dan berkomunikasi secara cerdas yang telah menjadi pionir dalam menggabungkan teknologi seperti kecerdasan buatan, analisis data tingkat tinggi, dan komputasi awan untuk mencapai potensi maksimal.

DAFTAR PUSTAKA

- Ariffudin, A., & Musa, P. (2022). Analisa sistem komunikasi data berbasis Internet of Things (IoT) menggunakan metode PIECES pada Sistem Pengamatan Cuaca Otomatis di Badan Meteorologi Klimatologi dan Geofisika (BMKG). *Jurnal Meteorologi dan Geofisika*, 23(2), 81. <https://doi.org/10.31172/jmg.v23i2.831>
- Asman, F. F., Permata, E., & Fatkhurrokhman, M. (2019). A Prototype of Smart Lock Based on Internet of Things (IoT) with ESP8266. *Jurnal Ilmiah Teknik Elektro Komputer Dan Informatika (JITEKI)*, 5(2), 101–111. <https://doi.org/10.26555/jiteki.v5i2.15317>
- Benomar, Z., Longo, F., Merlino, G., & Puliafito, A. (2021). Deviceless: A Serverless Approach for the Internet of Things. *2021 ITU Kaleidoscope: Connecting Physical and Virtual Worlds (ITU K)*, 1–8. <https://doi.org/10.23919/ITUK53220.2021.9662096>
- Dan, L., Xin, C., Chongwei, H., & Liangliang, J. (2015). Intelligent Agriculture Greenhouse Environment Monitoring System Based on IOT Technology. *2015 International Conference on Intelligent Transportation, Big Data and Smart City*, 487–490. <https://doi.org/10.1109/ICITBS.2015.126>
- Ebling, M. R. (2016). Pervasive Computing and the Internet of Things. *IEEE Pervasive Computing*, 15(1), 2–4. <https://doi.org/10.1109/MPRV.2016.7>
- Fruhlinger, J. (2022). *What is IoT? The internet of things explained*. Network World. <https://www.networkworld.com/article/963923/what-is-iiot-the-internet-of-things-explained.html>
- Gozali, F., Iskandardinata, R., Subrata, R. H., & Ferrianto Gozali Richard Iskandardinata, R. H. S. (2017). Sistem Pemantauan Dan Perekaman Gerak Kendaraan Secara Nirkabel Dengan Menggunakan Raspberry Pi. *Jurnal Teknologi Elektro*, 8(1), 9–15.
- Gudnyus.id, Gudnyus. id. (2019). *Perkembangan dan Manfaat Internet of Things (IoT)*.

- <https://www.gudnyus.id/2019/05/perkembangan-dan-manfaat-internet-of-things-iot.html>
- International Telecommunication Union, I. (2012). Overview of the Internet of things. *Series Y: Global Information Infrastructure, Internet Protocol Aspects and next-Generation Networks - Frameworks and Functional Architecture Models*.
- J. Showail, A. (2021). Internet of Things Security and Privacy. In F. Pedro García Márquez (Ed.), *Internet of Things*. IntechOpen. <https://doi.org/10.5772/intechopen.96669>
- Khan, M. A., & Salah, K. (2018). IoT security: Review, blockchain solutions, and open challenges. *Future Generation Computer Systems*, 82, 395–411.
- Kulkarni, P. (2022, September 26). *Evolution of Internet of Things (IoT)—A Brief History*. Bytebeam. <https://bytebeam.io/blog/a-brief-history-of-internet-of-things/>
- Kumar, S. (2021). *Fundamentals of Internet of Things* (1st ed.). Chapman and Hall/CRC. <https://doi.org/10.1201/9781003225584>
- Lee, I., & Lee, K. (2015). The Internet of Things (IoT): Applications, investments, and challenges for enterprises. *Business Horizons*, 58(4), 431–440.
- Madakam, S., Ramaswamy, R., & Tripathi, S. (2015). Internet of Things (IoT): A Literature Review. *Journal of Computer and Communications*, 03(05), 164–173. <https://doi.org/10.4236/jcc.2015.35021>
- Musa, P., Sugeru, H., & Mufza, H. F. (2019). An intelligent applied Fuzzy Logic to prediction the Parts per Million (PPM) as hydroponic nutrition on the based Internet of Things (IoT). *4th International Conference on Informatics and Computing (ICIC)*. <https://doi.org/10.1109/ICIC47613.2019.8985712>
- Park, C. S., & Nam, H. M. (2020). Security Architecture and Protocols for Secure MQTT-SN. *IEEE Access*. <https://doi.org/10.1109/ACCESS.2020.3045441>
- Pedro García Márquez, F. (Ed.). (2021). Introductory Chapter: Internet of Things. In *Internet of Things*. IntechOpen. <https://doi.org/10.5772/intechopen.98268>

- Sethi, P., & Sarangi, S. R. (2017). Internet of Things: Architectures, Protocols, and Applications. *Journal of Electrical and Computer Engineering*, 2017, 1–25. <https://doi.org/10.1155/2017/9324035>
- Wilianto, W., & Kurniawan, A. (2018). SEJARAH, CARA KERJA DAN MANFAAT INTERNET OF THINGS. *Matrix: Jurnal Manajemen Teknologi Dan Informatika*, 8(2), 36. <https://doi.org/10.31940/matrix.v8i2.818>
- Youssef, M., & Hassan, M. (2019). Next Generation IoT: Toward Ubiquitous Autonomous Cost-Efficient IoT Devices. *IEEE Pervasive Computing*, 18(4), 8–11. <https://doi.org/10.1109/MPRV.2019.2947974>
- Zou, W., Yao, F., Zhang, B., He, C., & Guan, Z. (2017). Verification and predicting temperature and humidity in a solar greenhouse based on convex bidirectional extreme learning machine algorithm. *Neurocomputing*, 249, 72–85. <https://doi.org/10.1016/j.neucom.2017.03.023>

BAB 2

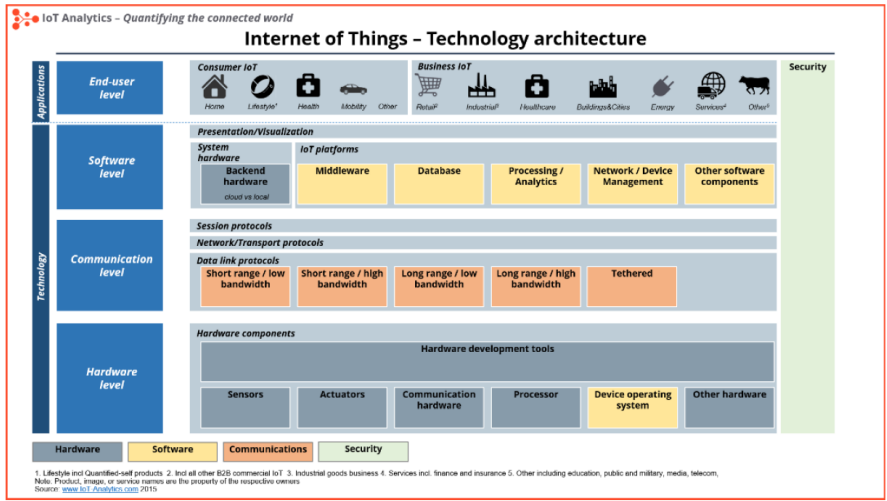
ARSITEKTUR IoT

Oleh Amin Ama Duwila

2.1 Pendahuluan

(Weber, 2010) menggambarkan Internet of Things adalah arsitektur layanan informasi berbasis Internet yang berkembang secara global.

Internet of Things dibangun di atas tiga lapisan teknologi utama yaitu *Hardware* (termasuk chip dan sensor), *Communication* (termasuk sebagian besar bentuk jaringan nirkabel), dan *Software* (termasuk penyimpanan data, analisis, dan aplikasi front end).(Lueth, 2015)



Gambar 2.1. IoT technology architecture
Sumber : (Lueth, 2015)

Definisi arsitektur suatu sistem menurut ISO/IEC/IEEE 42010:2011, adalah konsep atau sifat mendasar dari suatu sistem dalam lingkungannya yang diwujudkan dalam elemen, hubungan,

dan prinsip-prinsip desain dan evolusinya. Arsitektur mendefinisikan desain lengkap dari setiap teknologi, perangkat, atau perangkat komputasi apapun. Secara teknis, arsitektur mengacu pada hubungan fisik dan logis antara komponen-komponen tersebut. Arsitektur terdiri dari berbagai pedoman, prinsip, dan kerangka kerja untuk membangun sistem baru. Tujuan utama dari setiap arsitektur adalah untuk memberikan arahan yang tepat untuk mengumpulkan, membangun, mengimplementasikan, mengubah, dan menghubungkan berbagai sumber daya teknologi informasi.(Soni, 2022)

Arsitektur IoT adalah cara perangkat IoT terhubung, berkomunikasi, dan bekerja bersama untuk mencapai tujuan yang diinginkan. Arsitektur ini menyusun kerangka kerja yang mengintegrasikan perangkat fisik, perangkat lunak, dan jaringan untuk menciptakan sistem yang cerdas dan terintegrasi.(Indobot Academy, 2023) Dengan demikian arsitektur IOT merupakan struktur yang mencakup perangkat keras, perangkat lunak, komunikasi protokol dan keamanan yang diperlukan untuk mendukung pengoperasian perangkat yang berhubungan dalam jaringan IoT. Arsitektur IoT yang terdiri dari perangkat, struktur jaringan, dan teknologi cloud memungkinkan perangkat IoT berkomunikasi satu sama lain dengan tujuan utama adalah mengelola informasi yang dikumpulkan oleh teknologi yang mendukung IoT sehingga dapat dianalisis atau diproses sesuai kebutuhan. Tanpa arsitektur IoT yang tepat, jaringan akan menjadi tidak dapat diandalkan, sehingga menggagalkan seluruh tujuan investasi di IoT. Dengan demikian Arsitektur Internet of Things adalah konsep multidimensi, yang mencakup perangkat keras, perangkat lunak, protokol, dan standar(Raj, 2023)

(Oyalana, 2022) menguraikan bahwa Arsitektur IoT meningkatkan kemampuan bisnis yaitu dengan memahami pelanggan dengan lebih baik, menciptakan nilai tambah tools, mengoptimalkan operasi, dan monetise insight

Keberagaman perangkat, protokol jaringan, dan format data yang digunakan untuk solusi IoT merupakan tantangan arsitektur IoT, oleh karena penggunaan lebih dari satu platform IoT harus mempertimbangkan apakah teknologi yang digunakan dalam

setiap platform IoT dapat diintegrasikan ke dalam solusi yang kohesif.

Strategi yang membantu dalam menyederhanakan pengembangan, mengelola kompleksitas, dan memastikan solusi IoT tetap terukur, fleksibel, dan *robust* yaitu mengadopsi arsitektur berlapis, keamanan berdasarkan desain, mengotomatiskan operasi, desain untuk interoperabilitas dan ikuti arsitektur referensi.(Gerber, 2017)

2.2 Komponen Utama Arsitektur IoT

Komponen utama arsitektur IoT adalah sensor, aktuator, penyimpanan data, sistem kontrol, media komunikasi digital, dan aplikasi untuk tindakan berbasis informasi(Chaudhuri, 2019)

2.2.1 Sensor dan Aktuator

Sensor telah didefinisikan oleh IEEE sebagai “perangkat elektronik yang menghasilkan data listrik, optik, atau digital yang berasal dari kondisi atau peristiwa fisik. Data yang dihasilkan dari sensor kemudian ditransfer secara elektronik, oleh perangkat lain, menjadi informasi (output) yang berguna dalam pengambilan keputusan yang dilakukan oleh perangkat ‘cerdas’ atau individu (manusia).”

Aktuator didefinisikan sebagai “perangkat mekanis yang menerima sinyal data dan melakukan tindakan berdasarkan sinyal tersebut.”

2.2.2 Media Komunikasi Digital untuk IoT

Media komunikasi untuk 'Things' dapat berupa kabel atau nirkabel dan dapat dipilih dari berbagai protokol. Beberapa opsi komunikasi yang populer sebagai berikut :

1. Internet

Internet adalah media komunikasi digital yang paling populer. Internet Protokol Internet (IP) adalah "seperangkat aturan teknis yang mendefinisikan bagaimana komputer berkomunikasi melalui jaringan. " Dua versi IP yang saat ini digunakan adalah IP versi 4 (IPv4) dan IP versi 6 (IPv6).

2. 6LoWPAN

6LoWPAN (*IPv6 over Low power Wireless Personal Area Networks*), adalah protokol berbasis IPV6 yang memungkinkan perangkat dengan konsumsi daya kecil seperti sensor tetap dapat terkoneksi dan ikut berpartisipasi dalam IoT (Internet of things) dengan skalabilitas lebih besar. Teknologi jaringan ini memungkinkan paket IPV6 dibawa secara efisien oleh perangkat yang sesuai dengan standar IEEE 802.15.4. Perangkat jaringan 6LoWPAN dicirikan oleh jangkauannya yang pendek, kecepatan bit rendah dan konsumsi daya yang rendah

3. *Zigbee*

Zigbee adalah protokol komunikasi nirkabel yang sesuai dengan standar IEEE 802.15.4. Zigbee dapat digunakan dalam solusi IoT di dalam maupun di luar ruangan. Zigbee beroperasi pada pita radio 2,4 GHz, yang tersedia untuk digunakan secara global tanpa lisensi, sehingga aplikasi yang menggunakan Zigbee dapat dibawa ke lokasi global mana pun. Perangkat non-routing yang menggunakan standar Zigbee dapat berjalan dengan catu daya seperti baterai atau sel surya, atau dapat memanfaatkan Zigbee Green Power. Untuk transfer informasi yang aman dan melalui udara, Zigbee menggunakan enkripsi AES128.

4. *Bluetooth Low Energy (BLE)*

Bluetooth Low Energy (BLE) adalah jaringan area pribadi nirkabel yang beroperasi di 2.4 Spektrum GHz ISM dan dirancang untuk memungkinkan koneksi antar perangkat dalam jarak yang relatif pendek. BLE dapat mengaktifkan koneksi nirkabel short-burst di berbagai topologi jaringan, seperti topologi point-to-point (P2P) untuk komunikasi perangkat satu-ke-satu komunikasi perangkat, topologi siaran untuk komunikasi perangkat satu-ke-banyak atau topologi mesh untuk komunikasi banyak perangkat. BLE mendukung platform komputasi seluler utama seperti iOS, Android, Windows, Linux.

5. *LoRaWAN*

LoRaWAN (*Long Range Wide Area Network*) adalah protokol komunikasi nirkabel yang berbasis pada teknologi *Long Range*

(LoRa). LoRaWAN memungkinkan perangkat IoT terhubung ke jaringan secara nirkabel dengan jangkauan yang luas, dan hemat daya baterai. LoRaWAN menggunakan gateway untuk menyampaikan pesan di antara perangkat akhir dan server jaringan pusat. Pada LoRaWAN, perangkat akhir menggunakan komunikasi nirkabel single-hop, sementara gateway terhubung menggunakan koneksi IP standar.

6. *Modbus*

Modbus adalah protokol komunikasi serial untuk perangkat industri dan enabler untuk Industrial IoT (IIoT). Ini adalah protokol terbuka dan mengikuti model master-slave di mana perangkat 'master' meminta informasi dan perangkat 'slave' memasok informasi. Modbus dapat digunakan dalam kontrol pengawasan dan sistem akuisisi data.

7. *MQTT*

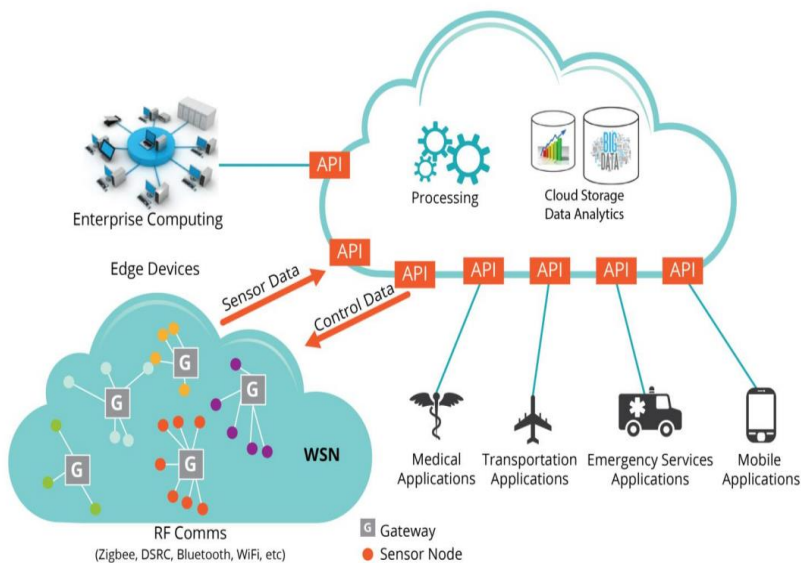
Message Queuing Telemetry Transport (MQTT) adalah suatu operasi terbuka dari machine-to-machine yang menghubungkan protokol untuk komunikasi IoT. Ini adalah protokol yang ringan, memiliki Broker MQTT sebagai mediator untuk berinteraksi dengan agen MQTT. Sistem kerja MQTT menerapkan *Publish* dan *Subscribe* data. Dan pada penerapannya, device akan terhubung pada sebuah Broker dan mempunyai suatu Topic tertentu.

8. *Cloud, Fog and Data Analytics*

Karena sensor mengumpulkan data kontekstual, berdasarkan desain dan arsitekturnya, data ini dapat diproses secara lokal pada perangkat pintar sampai batas tertentu atau dapat dibuang sesekali ke perangkat gateway untuk pemrosesan zona. Komputasi pada tepi suatu jaringan disebut sebagai komputasi 'tepi' atau 'kabut'. Data dari sensor dapat juga dapat dikirim ke lokasi penyimpanan dan pemrosesan berbasis cloud. Layanan awan dapat bisa bersifat publik, pribadi, atau hibrida komunal atau keduanya atau komunitas, berdasarkan pada arsitektur dan desain layanan pintar.

Tergantung pada kebutuhan layanan pintar yang diberikan, aplikasi IoT dapat diintegrasikan dengan data *analytic engine* untuk penyempurnaan dan kustomisasi keluaran aplikasi.

Misalnya, aplikasi IoT berbasis domain dapat diaktifkan dengan berbagai infrastruktur dan komponen fungsional, seperti sensor yang menangkap data kontekstual berdasarkan parameter yang telah ditentukan, perangkat gateway yang mengumpulkan data dari sekumpulan sensor, penyimpanan data yang dapat berada di tepi atau dihosting di cloud tempat gateway perangkat membuang data yang dikumpulkan secara berkala, fungsi pemrosesan analitis, fungsi bisnis berbasis antarmuka pemrograman aplikasi (API), perintah dan fungsi kontrol untuk aktuator dalam sensor, dan komunikasi jaringan kabel atau nirkabel menghubungkan komponen-komponen ini, seperti yang ditunjukkan pada Gambar 2.2.



Gambar 2.2. *Infrastructure and functional components for the Internet of Things.*

Sumber : (Cloud Security Alliance, 2015)

2.3 Lapisan Arsitektur IoT

Implementasi IoT didasarkan pada arsitektur yang terdiri dari beberapa lapis. Arsitektur berlapis harus dirancang sedemikian rupa sehingga dapat memenuhi kebutuhan pengguna. Tidak ada konsensus tunggal mengenai arsitektur untuk IoT, yang disepakati secara universal. Berbagai lapis arsitektur yang berbeda telah diusulkan oleh peneliti dan pengembang teknologi informasi. Berdasarkan kompleksitasnya, elemen sistem IoT dikelompokkan menjadi 3 hingga 7 lapis, yang masing-masing memiliki perannya sendiri.

2.3.1 Arsitektur 3 Lapis

Arsitektur Tiga lapis yang dijadikan sebagai dasar konsep, antara lain persepsi (*Perception/Device*), jaringan (*Network*), dan aplikasi (*Application*).

1. *Perception*

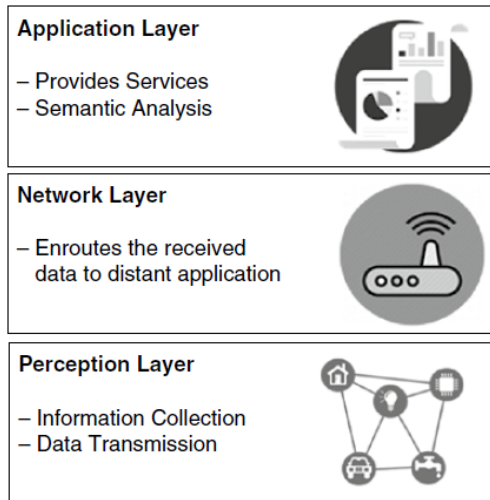
Perception merupakan lapis pertama dalam arsitektur IoT yang membahas mengenai komponen fisik dalam arsitektur. Contoh komponen tersebut adalah sensor, aktuator, atau perangkat apapun yang bersentuhan dengan lingkungan. Hal tersebut bertujuan agar perangkat dalam mengumpulkan semua informasi yang diperlukan dalam mendukung proyek yang sedang berjalan.

2. *Network*

Network merupakan suatu proses pengolahan berdasarkan pada data yang sudah terkumpul. Lapis network ini terhubung dengan beragam perangkat dan bertujuan untuk menjaga distribusi keseluruhan data.

3. *Application*

Lapis Aplikasi digunakan untuk berinteraksi dengan user. Contoh penerapan lapis aplikasi yaitu pada saat menekan tombol untuk mengoperasikan benda elektronik pada smart device.



Gambar 2.3. Arsitektur IoT - 3 Lapis
 Sumber : (Iqbal *et al.*, 2021a)

2.3.2 Arsitektur 5 Lapis

Arsitektur tiga lapis adalah cara yang bagus untuk menggambarkan proyek IoT, namun cakupannya agak terbatas. Karena alasan ini, banyak arsitektur yang diusulkan memiliki lapisan berbeda atau tambahan.

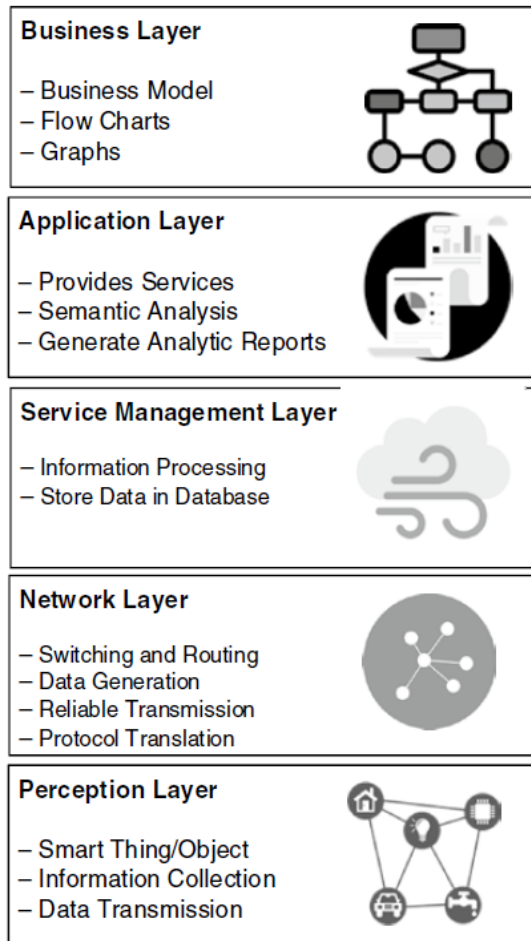
Melalui arsitektur teknologi dari Internet dan struktur logis jaringan manajemen telekomunikasi dan dikombinasikan dengan fitur-fitur spesifik dari Internet of Things, dikembangkan arsitektur Lima lapis(Wu *et al.*, 2010), yang terdiri atas Lapisan Bisnis (*Business Layer*), Lapisan Aplikasi (*Application Layer*), Lapis Manajemen Layanan (*Service Management Layer*), Lapis Jaringan (*Network Layer*) dan Lapis Persepsi (*Perception Layer*).

Selain lapisan Persepsi, jaringan dan Aplikasi yang sama, dua lapisan berikut yaitu :

1. *Service Management Layer (Middleware)* : Lapisan manajemen layanan menyediakan pemasangan layanan dengan aplikasi pemintanya dan memungkinkan pemrogram aplikasi IoT menangani data heterogen yang dibuat oleh objek pintar dengan spesifikasi perangkat keras

berbeda. Lapisan ini mencakup pemrosesan data yang diterima sebelum dikirim ke lapisan aplikasi.

2. *Business Layer* : Lapisan bisnis bertanggung jawab untuk mengelola keseluruhan aktivitas/layanan sistem IoT melalui pembuatan diagram alir, model bisnis, dan grafik pada data olahan yang diterima dari lapisan aplikasi. Selain itu, berdasarkan analisis Big Data, lapisan ini mendukung pengambilan keputusan otomatis serta pembuatan strategi bisnis yang cerdas.



Gambar 2.4. Arsitektur IoT – 5 Lapis
Sumber : (Iqbal *et al.*, 2021b)

2.3.3 Arsitektur 7 Lapis

Arsitektur 7 lapis representasi gabungan dari semua elemen yang tercakup dalam model sebelumnya. Arsitektur 7 lapis sebagai panduan untuk desain solusi IoT yang komprehensif. Lapisan model 7 lapis untuk arsitektur IoT meliputi *Perception layer, Connectivity layer, Edge computing layer, Processing layer, Application layer, Business layer dan Security layer*.

Lapisan keamanan (*security Layer*) merupakan tambahan dan terpenting dari arsitektur 7 lapis. Keamanan pada level perangkat (*device*) melibatkan integrasi perlindungan khusus dalam firmware dan perangkat keras untuk jaringan IoT. Keamanan pada level koneksi (*connectivity*) untuk IoT berfokus pada enkripsi data rahasia dengan bantuan protokol pesan aplikasi IoT. Selain itu, keamanan pada level cloud menekankan pada enkripsi data cloud untuk memastikan mitigasi risiko.

Tabel 2.1. Lapisan pada Arsitektur IoT

	3-layer	5-layer	7-layer	
Perception	+	+	+	The layer of physical devices, that gather information about the environment
Network	+	+	+	The layer is responsible for the communication within IoT (between smart things, gateway, the cloud)
Application	+	+	+	The layer where users interact with the IoT through the graphical user interface
Middleware (the cloud)	-	+	+	The layer is responsible for data storage, analysis, and management. It is enhanced by powerful analytic tools, Big Data algorithms, Machine learning.
Business	-	+	+	The layer where businesses manage the whole IoT system. It declares business goals and vital postulates that will become the basis for the

				IoT system.
Edge (or fog computing)	-	-	+	The layer performs data preprocessing before the information will be transferred to the cloud.
Security	-	-	+	The layer is responsible for access control to the IoT network, the security of data transfers, preventing data breaches, and tracking malicious software.

Sumber : (Sumatosoft, no date)

Cara lain untuk menggambarkan arsitektur solusi IoT adalah menggunakan pendekatan empat tahap. Pendekatan empat tahap memberikan penjelasan tentang berbagai komponen yang membentuk solusi IoT atau deskripsi strukturnya. Empat tahapan yang digunakan dalam arsitektur IoT :



Gambar 2.5. Komponen Pendekatan 4 Tahap

Sumber : (MongoDB, no date)

Devices : Tahap ini membahas tentang perangkat sebenarnya dalam solusi IoT. Perangkat ini bisa berupa sensor atau aktuator di lapisan Persepsi. Perangkat tersebut akan menghasilkan data (dalam kasus sensor) atau bertindak terhadap lingkungannya (dalam kasus aktuator). Data yang dihasilkan diubah dalam bentuk digital dan dikirimkan ke tahap gateway internet. Kecuali jika keputusan penting harus dibuat, data biasanya dikirim dalam keadaan mentah ke tahap berikutnya karena terbatasnya sumber daya perangkat itu sendiri.

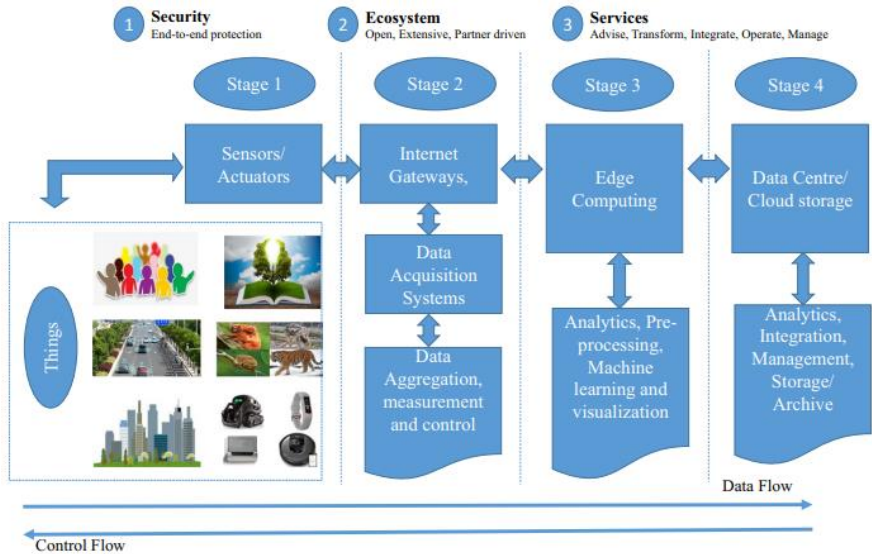
Beberapa contoh objek terhubung yang digunakan saat ini di berbagai industri yaitu :

1. Sensor IoT : sensor suhu, sensor GPS, sensor cahaya, sensor kelembaban, sensor jarak, dan lain-lain.
2. Aktuator: aktuator listrik, aktuator magnetik, aktuator pneumatik, aktuator termal, aktuator hidrolik, dan sebagainya

Internet Gateway : Tahap Internet Gateway akan menerima data mentah dari perangkat dan memprosesnya terlebih dahulu sebelum mengirimkannya ke cloud. Internet Gateway ini dapat dipasang secara fisik ke perangkat atau perangkat yang berdiri sendiri yang dapat berkomunikasi dengan sensor melalui jaringan berdaya rendah dan menyampaikan data ke internet.

Edge / fog computing : Untuk memproses data secepat mungkin bila ingin mengirim data ke edge cloud. Data akan dianalisis dengan cepat dan mengidentifikasi apakah ada sesuatu yang memerlukan perhatian segera. Lapisan ini biasanya hanya berkaitan dengan data terkini yang diperlukan untuk operasi yang memerlukan waktu kritis. Beberapa pra-pemrosesan mungkin dilakukan pada tahap ini juga, untuk membatasi data yang pada akhirnya ditransfer ke cloud.

Cloud / Data Center : Pada tahap akhir ini, data disimpan untuk diproses nanti. Lapisan aplikasi dan bisnis berada pada tahap ini, di mana dasbor atau perangkat lunak manajemen dapat dimasukkan melalui data yang disimpan di cloud. Analisis mendalam atau operasi intensif sumber daya seperti pelatihan pembelajaran mesin akan dilakukan pada tahap ini



Gambar 2.6. Arsitektur IoT empat tahap untuk data yang sangat besar

Sumber : (Kumar, Tiwari and Zymbler, 2019)

2.4 Arsitektur Referensi IoT

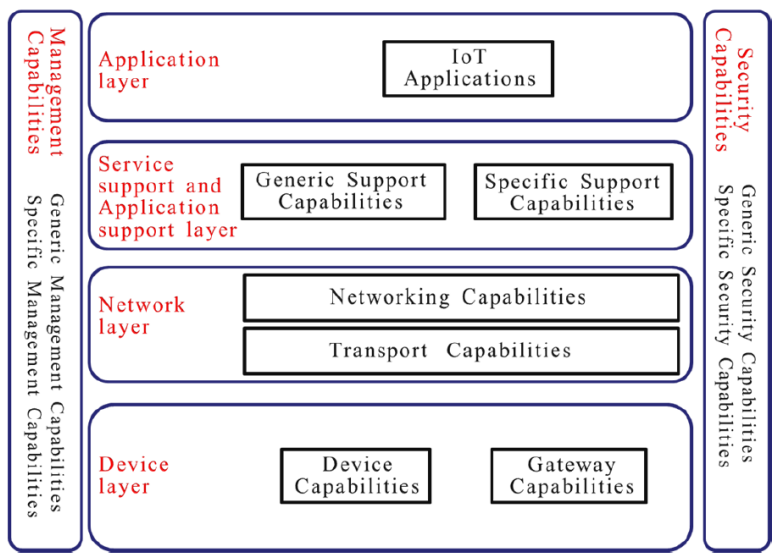
Arsitektur referensi IoT adalah kerangka kerja komprehensif yang berfungsi sebagai panduan untuk merancang dan mengimplementasikan solusi IoT. Arsitektur ini mendefinisikan komponen utama, interaksi, dan praktik terbaik untuk penerapan IoT. Arsitektur referensi ini berfungsi sebagai titik acuan untuk desain sistem IoT dan memastikan interoperabilitas dan skalabilitas. Arsitektur Referensi dapat membantu pengembang perangkat lunak IoT untuk memahami, membandingkan, dan mengevaluasi IoT yang berbeda dengan mengikuti suatu praktik yang seragam.

Beberapa Arsitektur Referensi telah diusulkan untuk menstandarkan konsep dan implementasi sistem IoT di domain yang berbeda.

2.4.1 Model Referensi IoT - ITU

Model Referensi *International Telecommunication Union* (ITU) terdiri dari empat lapisan yaitu application layer, service

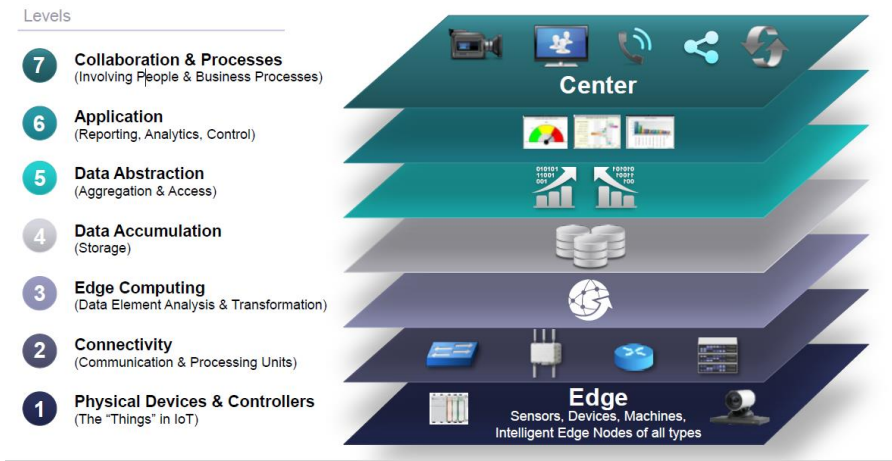
support and application support layer, network layer, dan device layer.



Gambar 2.7. ITU – IoT Reference Model
Sumber : (*Overview of the Internet of Things*, 2012)

2.4.2 Model Referensi IoT - CISCO

Model Referensi CISCO terdiri dari tujuh lapisan yaitu *Physical Devices & Controllers layer*, *Connectivity layer*, *Edge Computing layer*, *Data accumulation layer*, *Data abstraction layer*, *Application layer*, dan *Collaboration & Process layer*.



Gambar 2.8. CISCO – IoT Reference Model
Sumber : (CISCO, 2014)

Level 1: *Physical Devices and Controllers*

Perangkat fisik dan pengontrol adalah perangkat endpoint yang mengirim dan menerima informasi, dan merupakan 'Things' dalam IoT. Perangkat ini dapat dikendalikan melalui Internet dan mampu melakukan konversi sinyal analog ke digital dan menghasilkan data kontekstual. Karena daya komputasi dan penyimpanan yang rendah, perangkat akan mengeluarkan data yang diambil secara intermiten dalam unit-unit kecil ke jaringan peralatan di Level 2.

Level 2: *Connectivity*

Komunikasi dan konektivitas 'Things' dipertahankan pada tingkat ini untuk transmisi informasi yang andal dan tepat waktu. Informasi dapat mengalir di antara perangkat yang dapat diandalkan di Level 1 dan jaringan, di seluruh jaringan (lalu lintas timur-barat), dan antara jaringan (Level 2) dan pemrosesan informasi tingkat rendah yang terjadi di Level 3. Communication gateways dapat diterapkan untuk menghubungkan perangkat lama yang tidak mendukung IP. Beberapa aktivitas komputasi seperti menerapkan keamanan jaringan keamanan jaringan atau penerjemahan protokol dapat terjadi pada Level 2.

Level 3: *Edge (Fog) Computing*

Adanya persyaratan untuk konversi lokal aliran data jaringan menjadi informasi untuk memenuhi kebutuhan layanan IoT tertentu. Dalam situasi seperti ini, mengirimkan data kontekstual dari perangkat sensor ke 'cloud' terpusat untuk diproses dan ditindaklanjuti dapat menimbulkan beban operasional serta memakan waktu. Hal ini mengarah pada konsep komputasi 'edge' atau 'fog' untuk pemrosesan informasi sedekat mungkin dengan tepi jaringan, dengan latensi minimum dari pengambilan data.

Level 3 fokus pada aktivitas tersebut. Tugas komputasi seperti inspeksi pemeriksaan paket dapat dilakukan pada tingkat ini. Pemrosesan informasi terbatas dan dilakukan berdasarkan paket per paket. Pemrosesan informasi ini pada tingkat yang lebih tinggi dilakukan di Tingkat 4.

Level 4: *Data Accumulation*

Level 4 adalah tingkat penyimpanan di mana data berbasis peristiwa yang sedang bergerak dari jaringan diubah menjadi data diam untuk pemrosesan berbasis kueri oleh aplikasi bila diperlukan, secara *non-real time*. Beberapa aktivitas yang dilakukan pada tingkat ini meliputi pemfilteran/pengambilan sampel peristiwa, perbandingan peristiwa, agregasi peristiwa, dan peringatan (*alert*).

Level 5: *Data Abstraction*

Level ini membantu dalam agregasi data dari beberapa perangkat dan menyederhanakan akses data ke aplikasi dengan membuat skema dan tampilan data. Proses-proses utama pada level ini adalah penyaringan, pemilihan, proyeksi, dan rekonsiliasi data dalam format yang berbeda, konsistensi semantik data dari sumber yang berbeda, normalisasi / de-normalisasi dan pengindeksan data.

Level 6: *Application*

Semua jenis aplikasi berada pada tingkat ini, yang memberikan keluaran yang dirancang melalui interpretasi informasi yang tersedia, berupa aplikasi bisnis penting, aplikasi

seluler, laporan intelijen bisnis, analitik, aplikasi kontrol, dan sebagainya.

Level 7: *Collaboration and Processes*

Level ini berhubungan dengan orang-orang dan proses bisnis untuk komunikasi dan kolaborasi yang diperlukan agar aplikasi IoT bermanfaat

2.5 Persyaratan untuk Arsitektur IoT

Persyaratan utama untuk arsitektur IoT masa depan antara lain sebagai berikut : (Yaqoob *et al.*, 2017)

2.5.1 Kontrol Sumber Daya

Perangkat pintar yang berpartisipasi dalam lingkungan IoT harus dapat diakses dan dikonfigurasi secara jarak jauh. Dalam beberapa situasi, ketika administrator tidak tersedia di tempat tertentu mereka, mengendalikan sumber daya dari luar dapat membantu menyelesaikan masalah tersebut.

Selain itu, sistem IoT harus dapat menyeimbangkan beban jika terjadi ketersediaan sumber daya yang berlebihan yang dapat mengarah ke sumber daya yang tepat pemanfaatan sumber daya yang tepat.

2.5.2 Kesadaran Energi

Kesadaran energi diperlukan oleh karena sebagian besar perangkat memiliki keterbatasan sumber daya, dapat membantu menghemat konsumsi energi yang tidak perlu. Dalam beberapa kasus, ketika beban tidak terlalu banyak, perangkat harus mengubah diri sendiri ke *sleep mode*. Selain itu, pembentukan protokol komunikasi yang ringan dapat membantu menghemat energi perangkat pintar. Dengan demikian, arsitektur IoT harus dirancang sedemikian rupa sehingga dapat meminimalkan konsumsi energi.

2.5.3 Kualitas Layanan

Salah satu persyaratan arsitektur IoT adalah harus dapat memberikan kualitas layanan kepada pengguna. Kualitas layanan

dalam IoT dapat dipastikan dengan memprioritaskan layanan dan pengambilan. Aplikasi aplikasi yang membutuhkan *real-time processing* harus diberi prioritas tinggi untuk meningkatkan kinerjanya. Selain itu, dalam menanggapi *query*, hanya informasi yang diperlukan yang harus diambil.

2.5.4 Interoperabilitas

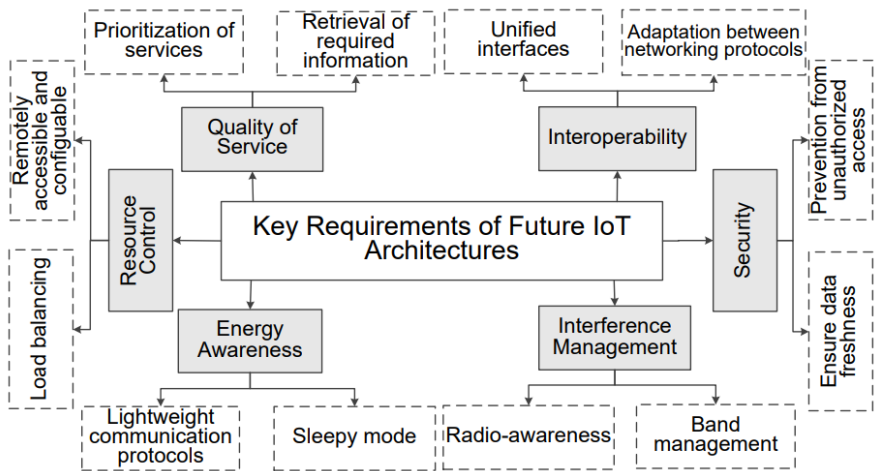
Dalam paradigma IoT, memungkinkan komunikasi di antara perangkat buatan vendor yang berbeda adalah salah satu persyaratan utama. Arsitektur IoT harus dapat mendukung jaringan internal dan komunikasi tanpa batas antara semua jenis aplikasi seperti aplikasi bisnis, desktop, dan mobile. Selain itu, untuk memungkinkan komunikasi antara perangkat yang dibatasi dan perangkat yang tidak dibatasi dari sistem IoT, adaptasi antara protokol jaringan harus diperlukan.

2.5.5 Manajemen interferensi

Arsitektur IoT harus mampu menangani masalah interferensi. Di masa depan, ketika sekian banyak perangkat pintar yang memiliki kemampuan multi-radio akan terhubung ke internet, interferensi akan menjadi masalah yang nyata. Konektivitas yang sempurna hanya dapat dipastikan dengan mengatasi masalah interferensi. Untuk mencapai layanan yang andal di lingkungan IoT, solusi bebas interferensi harus dikembangkan.

2.5.6 Keamanan

Arsitektur IoT harus aman untuk mencegah perangkat diaktifkan dengan cara yang tidak sah. Selain itu, mekanisme keamanan harus ringan karena sebagian besar perangkat memiliki keterbatasan sumber daya. Selain itu, memastikan kebaruan data juga sangat penting. Kurangnya dukungan keamanan yang kuat dalam IoT dapat merusak kepercayaan pengguna IoT yang dapat menyebabkan kegagalan teknologi.



Gambar 2.9. Persyaratan Utama Arsitektur IoT Masa Depan
 Sumber : (Yaqoob *et al.*, 2017)

DAFTAR PUSTAKA

- Chaudhuri, A. (2019) *Internet of things, for things, and by things*. CRC Press.
- CISCO (2014) *Internet of Things Reference Model*. Available at: http://cdn.iotwf.com/resources/71/IoT_Reference_Model_White_Paper_June_4_2014.pdf.
- Cloud Security Alliance (2015) *Guidance for early adopters of the internet of things*. Available at: [https:// Securitydownloads.cloudsecurityalliance.org/whitepapers/Security_Guidance_for_Early_Adopters_of_the_Internet_of_Things.pdf](https://Securitydownloads.cloudsecurityalliance.org/whitepapers/Security_Guidance_for_Early_Adopters_of_the_Internet_of_Things.pdf).
- Gerber, A. (2017) *Simplify the development of your IoT solutions with IoT architectures*, <https://developer.ibm.com/articles/iot-lp201-iot-architectures/>. Available at: <https://developer.ibm.com/articles/iot-lp201-iot-architectures/> (Accessed: 3 January 2024).
- Indobot Academy (2023) *Mengenal Arsitektur Internet of Things*, <https://blog.indobot.co.id/mengenal-arsitektur-internet-of-things/>.
- Iqbal, M. et al. (2021a) *Enabling the internet of things : fundamentals, design, and applications*. First Edition. John Wiley & Sons Ltd.
- Iqbal, M. et al. (2021b) *Enabling the internet of things : fundamentals, design, and applications*. First Edition. John Wiley & Sons Ltd.
- Kumar, S., Tiwari, P. and Zymbler, M. (2019) 'Internet of Things is a revolutionary approach for future technology enhancement: a review', *Journal of Big Data*, 6(1), p. 111. Available at: <https://doi.org/10.1186/s40537-019-0268-2>.
- Lueth, K.L. (2015) *IoT basics: Getting started with the Internet of Things*.
- MongoDB (no date) *What is IoT Architecture?* Available at: <https://www.mongodb.com/cloud-explained/iot-architecture> (Accessed: 13 January 2024).
- Overview of the Internet of Things (2012) *International Telecommunication Union*. International Telecommunication Union.

- Oyalana, M. (2022) *Why IoT architecture is essential to profitability*, https://blog.outvise.com/iot-architecture-is-essential-to-profitability/#How_the_Internet_of_Things_IoT_architecture_differs_from_the_Internet.
- Raj, A. (2023) *IoT Architecture - Detailed Explanation with Examples*, <https://www.almabetter.com/bytes/articles/iot-architecture>.
- Soni, V. (2022) *IoT for Beginners-Explore IoT Architecture, Working Principles, IoT Devices, and Various Real IoT Projects*. First Edition. India: BPB Publications.
- Sumatosoft (no date) *What is IoT Architecture - Advantages, Real-Life examples, Stages, Layers*, <https://sumatosoft.com/wp-content/uploads/2023/01/What-is-IoT-Architecture-SumatoSoft.pdf>.
- Weber, R.H. (2010) 'Internet of Things - New Security and Privacy Challenges', *Computer Law & Security Review*, 26, pp. 23–30.
- Wu, M. *et al.* (2010) 'Research on the architecture of Internet of things', *International Conference on Advanced Computer Theory and Engineering(ICAETE)*, pp. 484–487.
- Yaqoob, I. *et al.* (2017) 'Internet of Things Architecture: Recent Advances, Taxonomy, Requirements, and Open Challenges', *IEEE Wireless Communications*, 24(3), pp. 10–16.

BAB 3

PROTOKOL KOMUNIKASI DALAM IOT

Oleh Muhammad Irwan Syahib

3.1 Pendahuluan

Dalam dunia *Internet of Things*, protokol komunikasi bagaikan jembatan yang menghubungkan perangkat-perangkat, memungkinkan mereka untuk saling bertukar data dan berinteraksi. Memilih protokol yang tepat ibarat memilih kunci yang pas, memastikan kelancaran dan efisiensi komunikasi dalam jaringan IoT.

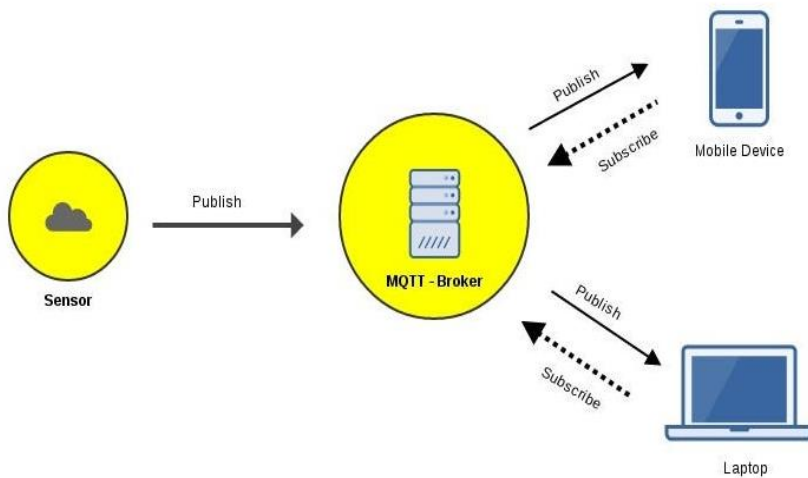
Bab ini mengupas beberapa protokol umum yang digunakan dalam IoT beserta keunggulannya masing-masing. Masing-masing protokol memiliki karakteristik unik, bagaikan pahlawan dengan kekuatan dan kelemahannya sendiri.

3.2 Jenis-jenis Protokol Komunikasi IoT

3.2.1 Message Queuing Telemetry Transport

Message Queuing Telemetry Transport yang disingkat MQTT adalah protokol pertukaran pesan yang dirancang khusus untuk komunikasi antar perangkat dalam *Internet of Things* (IoT). Keunggulan utama MQTT terletak pada aspek kemudahan dan keandalan. Protokol ini sangat ideal untuk perangkat dengan sumber daya terbatas karena konsumsi memorinya yang kecil dan penggunaan *bandwidth* yang minimal. Selain itu, arsitektur *publish-subscribe* pada MQTT memastikan pesan terkirim dengan sukses kepada penerima yang dituju, bahkan dalam kondisi jaringan yang tidak stabil. Oleh karena itu, MQTT menjadi pilihan tepat untuk membangun komunikasi yang hemat daya dan andal dalam berbagai aplikasi IoT.

Sistem kerja MQTT menerapkan *Publish* dan *Subscribe* data. Pada penerapannya *device* akan terhubung pada sebuah Broker dan mempunyai suatu topik tertentu.



Gambar 3.1. Protokol MQTT
(Sumber : <https://miro.medium.com>)

Pada gambar 3.1 dapat dilihat terdapat Broker pada MQTT yang berfungsi *menghandle* data *publish* dan *subscribe* dari berbagai device, bisa diibaratkan sebagai server yang memiliki alamat IP khusus. Beberapa contoh dari Broker yang ada seperti Mosquitto, HiveMQ dan Mosca. Sementara publish sendiri merupakan cara suatu device untuk mengirimkan datanya ke *subscribers*. Biasanya pada *publisher* ini terdapat sebuah device yang terhubung dengan sensor tertentu. Setiap sensor akan terhubung ke sebuah *gateway* seperti Ethernet shield, ESP8266, SIM800L atau device sejenisnya yang dapat menghubungkannya ke MQTT Broker. Antara *gateway* dan sensor terdapat *controller*, beberapa *controller* yang banyak digunakan seperti Arduino, RaspberryPi atau sejenisnya.

MQTT memiliki beberapa keunggulan yang perlu diketahui agar penggunaannya tepat sasaran:

1. Ringan

MQTT dirancang untuk perangkat dengan sumber daya terbatas, sehingga konsumsi memorinya kecil dan *bandwidth* yang digunakan minimal.

2. Andal
Arsitektur publish-subscribe memastikan pesan terkirim dengan sukses kepada penerima yang dituju, bahkan dalam kondisi jaringan yang tidak stabil.
3. Skalabilitas
MQTT mampu menangani komunikasi antar banyak perangkat secara efisien, membuatnya ideal untuk jaringan IoT yang besar.
4. Decoupling
Arsitektur decoupled memungkinkan perangkat untuk terhubung dan terputus tanpa mengganggu komunikasi perangkat lain.
5. Keamanan
MQTT dapat diamankan dengan mekanisme seperti TLS/SSL untuk komunikasi terenkripsi.

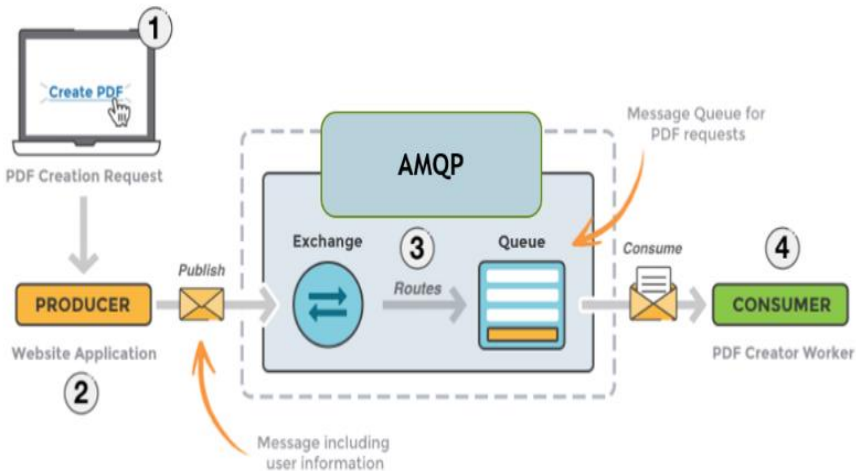
3.2.2 Advanced Message Queuing Protocol

Advanced Message Queuing Protocol yang disingkat AMQP adalah protokol komunikasi yang dirancang untuk memastikan pengiriman data yang handal dan efisien antar perangkat dalam *Internet of Things*. AMQP berfungsi sebagai perantara antara perangkat pengirim dan penerima pesan, memastikan pesan terkirim dengan aman dan tepat waktu. AMQP ini sering digunakan dalam berbagai aplikasi IoT diantaranya:

1. *Smart Grid*
AMQP digunakan untuk mengelola aliran data antar perangkat dalam jaringan *smart grid*, seperti meteran energi, sensor, dan turbin angin.
2. Manufaktur
AMQP digunakan untuk menghubungkan mesin dan sensor di pabrik, memungkinkan transfer data *real-time* untuk pemantauan dan kontrol proses produksi.
3. *Smart city*
AMQP digunakan untuk mengelola berbagai perangkat di *smart city*, seperti lampu jalan, sensor parkir, dan sistem keamanan.

4. Kesehatan

AMQP digunakan untuk menghubungkan perangkat medis dan aplikasi kesehatan, memungkinkan transfer data pasien dan pemantauan kesehatan jarak jauh.



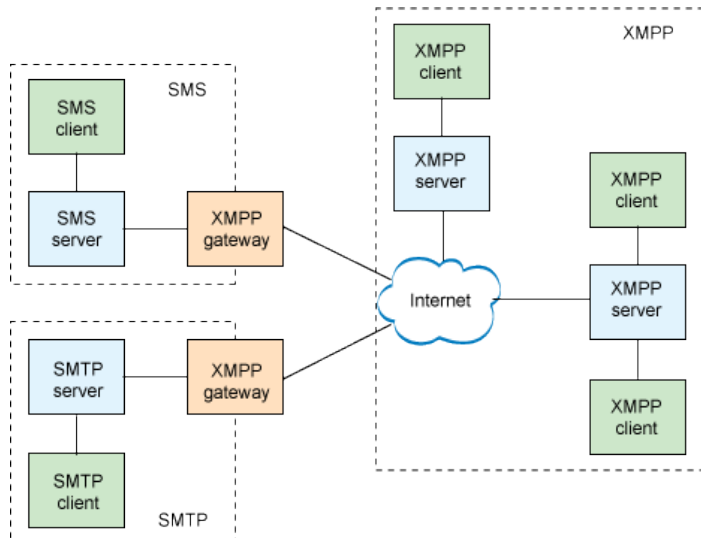
Gambar 3.2. Protokol AMQP
(Sumber : googleusercontent.com)

Perjalanan data dimulai dari perangkat IoT, seperti sensor atau aktuator, yang menghasilkan data berharga. Data ini dikemas menjadi pesan AMQP oleh sang publisher, aplikasi atau perangkat yang bertugas mengantarkannya. Pesan ini, bak ibarat pos, membawa informasi penting untuk diterima oleh pihak yang tepat. *Exchange* atau sang penentu arah menerima pesan dan menggunakan routing key, ibarat alamat surat, untuk menentukan tujuannya. Pesan diarahkan ke *queue*, tempat penyimpanan sementara, diibaratkan seperti kotak pos yang menunggu pengambilan. Selanjutnya *consumer* atau sang penerima mengambil pesan dari queue dan memprosesnya dengan cermat. Data diubah menjadi tindakan, seperti menyimpan informasi ke *database*, mengirimkan notifikasi, atau mengendalikan perangkat lain. Alur kerja ini memastikan setiap pesan diproses dengan sempurna. Setelah proses tersebut lalu konfirmasi pun dapat diberikan, ibarat

tanda terima surat, untuk memastikan pesan telah diterima dan diproses dengan sukses. AMQP, dengan fleksibilitasnya, memungkinkan berbagai mode pengiriman pesan, seperti *publish/subscribe* dan *request/reply*, untuk memenuhi kebutuhan komunikasi yang beragam. Kemampuan AMQP tak berhenti di situ. Protokol ini menjamin skalabilitas, memungkinkan jaringan IoT berkembang pesat tanpa hambatan. Keamanan pun tak luput dari perhatian, dengan enkripsi terintegrasi untuk melindungi data sensitif. Hal ini dapat disimpulkan bahwa AMQP adalah maestro orkestra di balik harmoni komunikasi IoT. Alur kerjanya yang terstruktur, fleksibel, dan aman menjadikannya pilihan tepat untuk membangun jaringan IoT yang andal dan dinamis.

3.2.3 Extensible Messaging and Presence Protocol

Extensible Messaging and Presence Protocol atau disingkat XMPP adalah protokol komunikasi real-time yang terbuka dan terdesentralisasi. XMPP digunakan untuk perpesanan instan, konferensi web, berbagi file, dan banyak lagi. Protokol ini memungkinkan pengguna untuk berkomunikasi satu sama lain secara langsung, tanpa memerlukan server pusat.



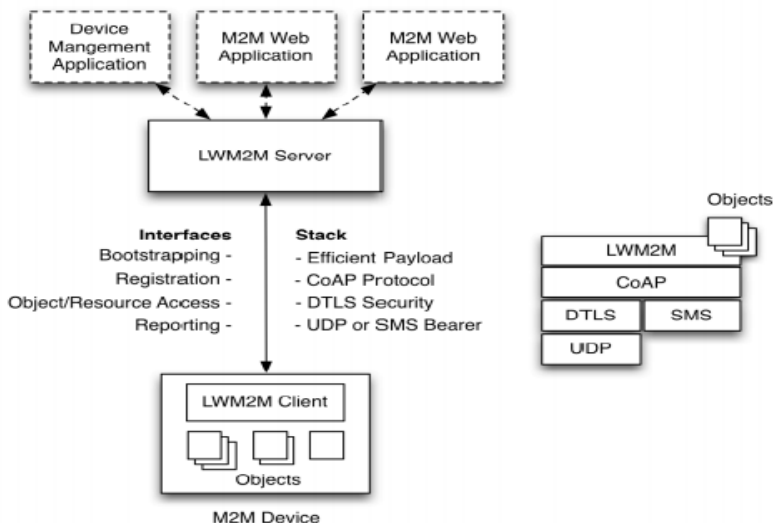
Gambar 3.3. Protokol XMPP
(Sumber : developer.ibm.com)

XMPP memiliki beberapa kelebihan dibandingkan protokol komunikasi lainnya, seperti:

1. Merupakan protokol open-source, yang berarti bahwa spesifikasi protokol tersedia secara bebas dan dapat digunakan oleh siapa saja.
2. Tidak memiliki server pusat, yang berarti bahwa jaringan XMPP tidak dapat dimatikan oleh satu entitas pun.
3. Dapat digunakan untuk berbagai aplikasi, seperti perpesanan instan, konferensi web, dan berbagi file.
4. Mendukung enkripsi dan autentikasi, yang membantu melindungi privasi dan keamanan pengguna.
5. Skalabel artinya mendukung jaringan pengguna dengan ukuran berapa pun.

3.2.4 Lightweight Machine to Machine

Lightweight Machine to Machine yang disingkat LwM2M adalah protokol komunikasi yang dirancang khusus untuk perangkat *Internet of Things* dengan sumber daya terbatas, seperti sensor, aktuator, dan gateway. Protokol ini ringan, hemat daya, dan mudah digunakan, sehingga ideal untuk perangkat IoT yang beroperasi di jaringan dengan *bandwidth* rendah.



Gambar 3.4. Protokol LwM2M
(Sumber : researchgate.net)

Protokol LwM2M bekerja dengan cara yang terstruktur dan terorganisir. Alurnya dimulai dengan perangkat LwM2M yang terhubung ke server LwM2M. Dalam proses ini, perangkat LwM2M mendaftarkan diri ke server, memberikan informasi penting tentang dirinya sendiri, seperti model dan kemampuannya. Informasi ini kemudian disimpan oleh server LwM2M dan digunakan untuk membuat model perangkat virtual yang merepresentasikan perangkat fisik. Komunikasi dua arah pun terjalin. Perangkat LwM2M secara berkala mengirimkan data dan statusnya ke server LwM2M, memungkinkan server untuk memantau dan memperbarui informasi tentang perangkat. Server LwM2M, di sisi lain, memiliki kemampuan untuk mengirim perintah ke perangkat LwM2M. Perintah-perintah ini dapat digunakan untuk mengontrol operasi perangkat, seperti menyalakan atau mematikan sensor, mengubah pengaturan, atau memulai proses tertentu. Pengguna berperan penting dalam mengelola dan memantau perangkat LwM2M. Mereka dapat melakukannya melalui klien LwM2M, yang menyediakan antarmuka untuk melihat data perangkat, mengontrol operasinya, dan melakukan konfigurasi yang diperlukan. Alur kerja ini memastikan komunikasi yang efisien dan terkontrol antara perangkat LwM2M, server LwM2M, dan pengguna, memungkinkan pengelolaan dan pemantauan perangkat IoT dengan mudah dan efektif.

Protokol LwM2M memiliki beberapa kelebihan dibandingkan protokol M2M lainnya, seperti:

1. Ringan, artinya LwM2M dirancang untuk perangkat dengan sumber daya terbatas, sehingga protokol ini ringan dan hemat daya.
2. Mudah digunakan artinya mudah diimplementasikan dan digunakan, sehingga ideal untuk pengembang yang ingin dengan cepat menambahkan konektivitas M2M ke perangkat mereka.
3. Mendukung enkripsi dan autentikasi, sehingga membantu melindungi privasi dan keamanan data.
4. Skalabilitas, yang artinya LwM2M dapat di-skala untuk mendukung jaringan perangkat dengan ukuran berapa pun.

3.2.5 Bluetooth

Bluetooth adalah teknologi komunikasi nirkabel jarak pendek yang memungkinkan perangkat elektronik untuk terhubung dan bertukar data tanpa memerlukan kabel. Teknologi ini menggunakan gelombang radio frekuensi tinggi 2.4 GHz untuk mentransfer data dalam jarak yang pendek, biasanya sekitar 10 meter.

Protokol *Bluetooth* tersusun atas beberapa lapisan yang bekerja sama untuk memungkinkan komunikasi nirkabel yang efektif antara perangkat. Berikut adalah penjelasan singkat dari setiap lapisan:

1. Radio

Lapisan radio adalah fondasi, menangani modulasi dan demodulasi sinyal radio. Di sinilah sinyal digital diubah menjadi gelombang radio dan sebaliknya, memungkinkan transmisi data melalui udara.

2. *Baseband*

Lapisan Baseband berperan penting dalam mengelola aspek fundamental komunikasi *Bluetooth*. Lapisan ini menangani kontrol akses, memastikan hanya satu perangkat yang dapat memancarkan pada waktu tertentu untuk menghindari tabrakan data. Selain itu, baseband bertanggung jawab untuk sinkronisasi perangkat dan enkripsi data untuk menjaga keamanan komunikasi.

3. LMP (*Link Manager Protocol*)

Lapisan LMP bertugas membangun dan mengelola tautan antara perangkat *Bluetooth*. LMP menangani proses penemuan perangkat, pembentukan koneksi, dan negosiasi parameter penting seperti tingkat daya dan jenis layanan yang didukung.

4. L2CAP (*Logical Link Control and Adaptation Protocol*)

Lapisan L2CAP menyediakan layanan penting untuk protokol tingkat atas. L2CAP memungkinkan multiplexing, di mana beberapa koneksi logis dapat berjalan secara bersamaan pada satu tautan fisik. Lapisan ini juga menangani fragmentasi dan penyusunan kembali data, memastikan pengiriman data yang andal.

5. *Profile*

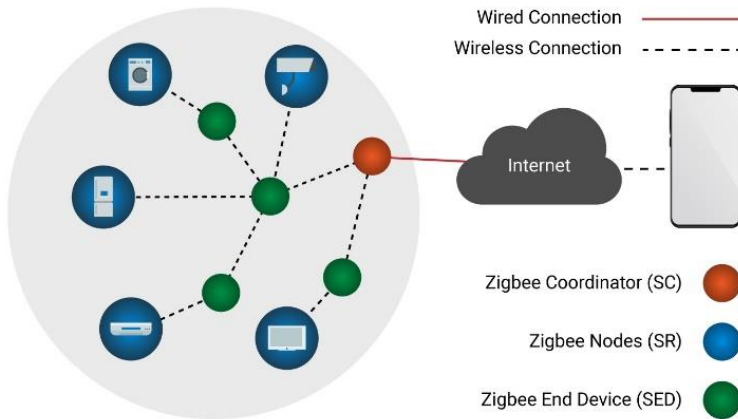
Lapisan *profile Bluetooth* mendefinisikan format data dan aturan komunikasi untuk aplikasi tertentu, seperti transfer file OBEX, audio A2DP, dan kontrol perangkat HID. *Profile* ini memungkinkan interoperabilitas antara perangkat yang mendukung aplikasi yang sama.

Dengan arsitektur berlapis diatas, protokol bluetooth mencapai keseimbangan antara kompleksitas dan fungsionalitas, memungkinkan komunikasi nirkabel yang mulus dan serbaguna untuk berbagai macam perangkat dan aplikasi.

Ada beberapa kelebihan yang dimiliki oleh *protocol* ini, diantaranya; *bluetooth* sangat ideal untuk koneksi jarak pendek antara perangkat pribadi, seperti *smartphone*, tablet, dan *headphone*. Selain itu *bluetooth* menggunakan daya yang rendah, sehingga perangkat *Bluetooth* dapat beroperasi dengan baterai selama berjam-jam. Selain hemat daya *Bluetooth* juga mudah dikonfigurasi dan digunakan, memungkinkan koneksi cepat dan mudah antara perangkat. Ditambah lagi *protocol* ini sudah menjadi standar global yang didukung oleh berbagai macam perangkat dari berbagai produsen dan sangat aman yang artinya bluetooth mendukung enkripsi dan autentikasi untuk melindungi data dari akses yang tidak sah.

3.2.6 *Zigbee*

Zigbee adalah protokol jaringan nirkabel jarak pendek yang dirancang untuk aplikasi *Internet of Things*. Teknologi ini menggunakan frekuensi radio pita rendah 2.4 GHz atau 868 MHz untuk memungkinkan komunikasi antara perangkat IoT dengan konsumsi daya yang rendah dan jangkauan yang moderat.



Gambar 3.5. Arsitektur Zigbee
(Sumber : <https://spikebot.io/>)

Jaringan *Zigbee* memiliki arsitektur yang terdiri dari tiga jenis perangkat, yaitu:

1. *Coordinator*

Coordinator ini berperan sebagai router utama, coordinator bertanggung jawab untuk membentuk dan mengelola jaringan *Zigbee*. Perangkat ini menginisiasi jaringan, menetapkan parameter jaringan, dan mengizinkan perangkat lain untuk bergabung.

2. Router

Perangkat ini berfungsi untuk memperluas jangkauan jaringan dengan meneruskan sinyal dari perangkat *Zigbee* lain. Router memperkuat sinyal dan memastikan data dapat mencapai semua perangkat di jaringan.

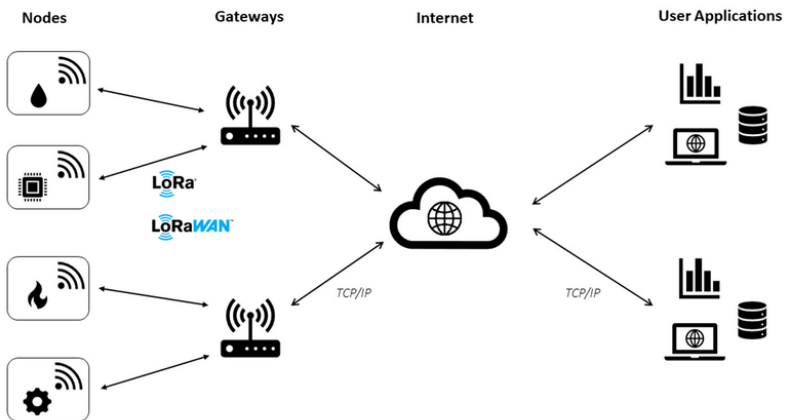
3. *End Device*

Berbeda dengan router, *end device* tidak dapat meneruskan sinyal. Perangkat ini hanya dapat berkomunikasi dengan *coordinator* atau router untuk mengirim dan menerima data. *End device* umumnya adalah sensor, aktuator, atau perangkat IoT lainnya yang perlu terhubung ke jaringan.

Kombinasi dari ketiga jenis perangkat tersebut memungkinkan *Zigbee* membangun jaringan yang skalabel dan fleksibel yang dapat menampung berbagai macam perangkat IoT. *Coordinator* memastikan kelancaran operasi jaringan, router memperluas jangkauan, dan end device menyediakan konektivitas untuk sensor dan perangkat IoT lainnya.

3.2.7 LoRa dan LoRaWAN

Long Range yang disingkat LoRa dan *Long Range Wide Area Network* yang disingkat LoRaWAN adalah dua teknologi yang saling terkait yang dirancang untuk komunikasi nirkabel jarak jauh dalam jaringan *Internet of Things*. LoRa adalah lapisan fisik yang menyediakan modulasi spread spectrum frekuensi rendah untuk komunikasi nirkabel yang hemat daya dan tahan interferensi. Sementara LoRaWAN adalah lapisan jaringan di atas LoRa yang menyediakan struktur jaringan, manajemen perangkat, dan autentikasi untuk komunikasi IoT yang aman dan andal.



Gambar 3.6. Arsitektur LoRa dan LoRaWAN
(Sumber : thethingsnetwork.org)

Berdasarkan Gambar diatas, cara kerja LoRa dan LoRaWAN dibagi beberapa bagian diantaranya:

1. *End Device*

Perangkat akhir adalah perangkat IoT yang ingin terhubung ke jaringan LoRaWAN. Perangkat ini dilengkapi dengan chip LoRa yang memungkinkan mereka untuk mengirim dan menerima data nirkabel. Perangkat akhir secara berkala mengirimkan paket data ke jaringan LoRaWAN. Paket data ini berisi informasi seperti sensor *readings*, status perangkat, atau perintah kontrol.

2. *Gateway LoRaWAN*

Gateway LoRaWAN adalah infrastruktur jaringan yang menghubungkan perangkat akhir ke jaringan IP. *Gateway* ini dilengkapi dengan antena LoRa yang memungkinkan mereka untuk menerima dan meneruskan sinyal LoRa dari perangkat akhir. *Gateway LoRaWAN* menerima paket data dari perangkat akhir dan meneruskannya ke server jaringan LoRaWAN.

3. *Server Jaringan LoRaWAN*

Server jaringan LoRaWAN adalah pusat kendali jaringan LoRaWAN. Server ini bertanggung jawab untuk:

- a. Menerima paket data dari gateway LoRaWAN.
- b. Memproses paket data untuk mengekstrak informasi yang berguna.
- c. Menyimpan data dalam database.
- d. Menyediakan akses ke data melalui API (*Application Programming Interface*).

4. *Aplikasi LoRaWAN*

Aplikasi LoRaWAN adalah perangkat lunak yang menggunakan data dari server jaringan LoRaWAN untuk menyediakan berbagai layanan. Aplikasi ini dapat digunakan untuk memantau data sensor dari perangkat akhir, mengontrol perangkat IoT, serta menganalisis data untuk mendapatkan wawasan.

DAFTAR PUSTAKA

- Culler, D. E., Estrin, D., Srivastava, M., & Sukhatme, B. (2004). Sensor Networks for Information Discovery. Elsevier.
- Miorandi, D., & Ho, D. (2016). Network Design and Management for the Internet of Things. Elsevier.
- Suo, T., Simon, G., & Zhou, Z. (2012). Wireless Sensor Networks: Architectures and Protocols. John Wiley & Sons.
- Yuandi, I.A., Amir, A.A., Syahib, M.I., Masri, F. and Saputra, S.R., 2024. Mitigating land fire disasters: Implementation of agricultural land fire risk management information system in Aunupe Village, South Konawe Regency. *Community Empowerment*, 9(2), pp.216-224.
- Zorzi, M., Gluhak, A., & Reddy, S. (2014). Contexts in the Internet of Things: Sensor data and information fusion. Springer.

BAB 4

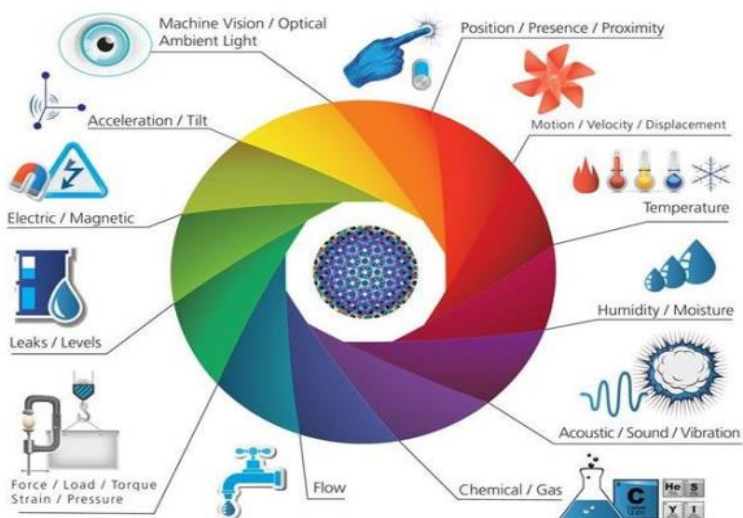
SENSOR DAN AKTUATOR PADA IOT

Oleh Alex Copernikus Andaria

4.1 Pendahuluan

Internet of Things merupakan salah satu penemuan yang dikembangkan dan berkembang pesat pada saat ini, karena memiliki kelebihan dari segi fungsionalitas dan efisiensi guna mendukung kerja dan pekerjaan melalui jaringan.

Internet of Things atau biasa disingkat IoT adalah konsep atau program yang mana sebuah objek memiliki kemampuan untuk mengirim atau mentransmisikan data melalui jaringan tanpa bantuan perangkat komputer maupun bantuan dari manusia. IoT (*Internet Of Things*) menjelaskan bahwa *internet of things* adalah suatu keadaan ketika benda memiliki identitas, bisa beroperasi secara intelijen, serta bisa berkomunikasi dengan sosial, lingkungan, dan penggunanya (Andaria *et al.*, 2023).



Gambar 4.1. Contoh Sensor Dalam Perangkat IoT
(Sumber : Nugroho, Prathivi and Daru, 2019)

Sensor yang dibutuhkan dalam perangkat IoT seperti yang terlihat pada gambar 4.1 dapat terdiri dari berbagai macam teknologi sensor. Integrasi setiap sensor yang akurat menjadikan teknologi IoT memiliki akurasi data yang tinggi (Nugroho , Prathivi and Daru, 2019).

4.2 Sensor dalam IoT

Sensor dalam *Internet of Things* (IoT) dapat diartikan perangkat yang mampu mendeteksi, mengukur, dan mengumpulkan data dari lingkungan fisik atau objek, lalu mentransmisikan informasi tersebut ke jaringan IoT untuk analisis lebih lanjut. Sensor dalam *Internet of Things* (IoT) berperan kritis dalam mengumpulkan data dari lingkungan fisik untuk mendukung fungsi dan aplikasi yang beragam.

4.2.1 Jenis dan Fungsi Sensor pada IoT

Pada Tabel 4.1, dijelaskan jenis jenis sensor, deskripsi, dan penerapan lingkungan, berdasarkan fungsi secara terperinci.

Tabel 4.1. Jenis-Jenis Sensor pada IoT berdasarkan fungsi

No.	Jenis Sensor	Deskripsi fungsi	Penerapan Lingkungan
1	Sensor Suhu	Mengukur suhu di sekitar.	Monitoring suhu udara, air, atau tanah.
2	Sensor Kelembaban	Mengukur tingkat kelembaban udara atau tanah.	Monitoring kelembaban udara, tanah pertanian, atau dalam aplikasi hortikultura.
3	Sensor Cahaya (Luminosity)	Mendeteksi intensitas cahaya di sekitar.	Pemantauan pencahayaan alami, sistem penerangan otomatis, atau penelitian ekologi.
4	Sensor Kualitas	Mendeteksi tingkat polutan di udara	Penerapan Lingkungan:

No.	Jenis Sensor	Deskripsi fungsi	Penerapan Lingkungan
	Udara	seperti partikel debu atau gas berbahaya.	Pemantauan kualitas udara di dalam dan di luar ruangan.
5	Sensor Gas	Mendeteksi dan mengukur konsentrasi gas tertentu di udara.	Penerapan Lingkungan: Pemantauan gas rumah tangga, pemantauan kualitas udara industri, atau deteksi kebocoran gas.
6	Sensor Tekanan (Pressure)	Mengukur tekanan udara atau fluida.	Pemantauan perubahan tekanan atmosfer, aplikasi meteorologi, atau pemantauan tinggi air.
7	Sensor Kecepatan Angin	Mengukur kecepatan angin.	Monitoring cuaca, penelitian meteorologi, atau aplikasi energi terbarukan.
8	Sensor Cuaca	Mengukur parameter cuaca seperti suhu, kelembaban, tekanan udara, dan kecepatan angin.	Pemantauan kondisi cuaca secara keseluruhan.
9	Sensor Suara (Sound)	Mendeteksi tingkat kebisingan atau suara di lingkungan	Pemantauan tingkat kebisingan perkotaan, penelitian ekologi suara, atau pemantauan keamanan.
20	Sensor Radiasi UV	Mendeteksi tingkat radiasi ultraviolet	Pemantauan paparan UV, kualitas radiasi matahari, atau untuk

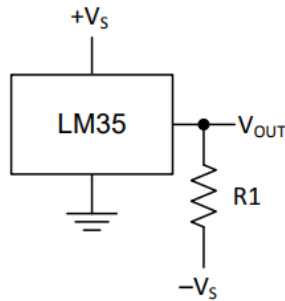
No.	Jenis Sensor	Deskripsi fungsi	Penerapan Lingkungan
			melindungi kulit manusia.
11	Sensor Keberadaan Partikel	Mendeteksi partikel debu atau polusi udara.	Pemantauan kualitas udara di daerah perkotaan atau industri.

Sumber: (Andaria *et al.*, 2023)

4.2.2 Karakteristik Sensor Suhu pada IoT

Sensor Suhu, pada IoT merupakan perangkat elektronik yang dirancang khusus untuk mengukur suhu lingkungan sekitarnya dan mentransmisikan data suhu secara nirkabel melalui jaringan Internet, memungkinkan pengguna untuk memantau dan mengendalikan suhu di berbagai lingkungan, seperti rumah, kantor, atau fasilitas industri, dari jarak jauh melalui perangkat seluler atau komputer. Dengan data suhu yang terus-menerus dipantau, sensor suhu pada IoT memungkinkan pengguna untuk mengoptimalkan efisiensi energi, memantau keamanan dan kenyamanan, serta mendeteksi kondisi lingkungan yang abnormal secara *real-time*.

Komponen LM35, Seri LM35 adalah sirkuit terpadu dengan pengukuran suhu yang presisi, yang tegangan keluarannya berbanding lurus dengan suhu Celcius. Dengan Fitur umum : Rentang suhu: -55°C hingga +150°C; Akurasi: $\pm 0.5^{\circ}\text{C}$ pada suhu ruangan; Tegangan operasi: 4V hingga 30V (Texas Instruments, 2017).



Choose $R_1 = -V_s / 50 \mu A$
 $V_{OUT} = 1500 \text{ mV at } 150^\circ C$
 $V_{OUT} = 250 \text{ mV at } 25^\circ C$
 $V_{OUT} = -550 \text{ mV at } -55^\circ C$

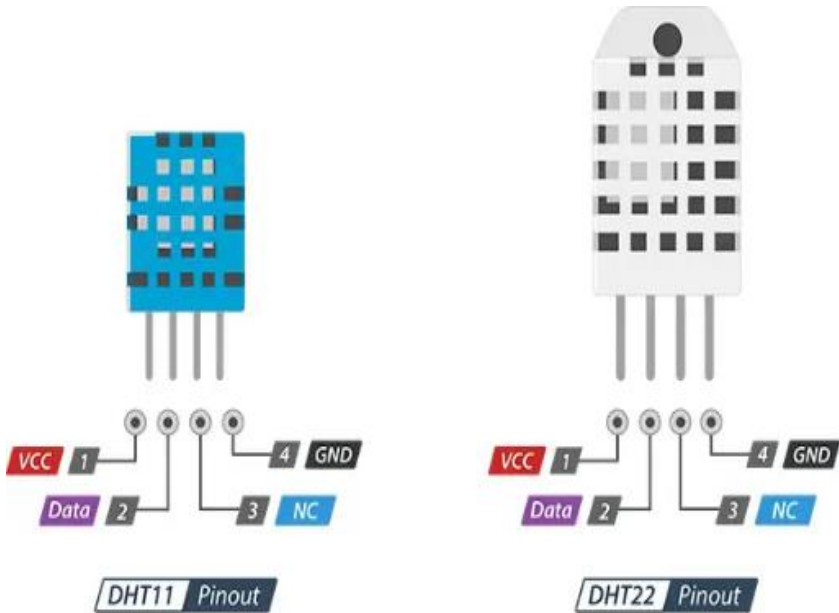
Gambar 4.2. LM35 Jangkauan Penuh
 (Sumber : Texas Instruments, 2017)

Modul DHT11 dan Modul DHT22 (disebut juga AM2302), keduanya merupakan modul sensor kelembaban dan suhu, perbedaan kedua modul ini dapat dilihat pada tabel 4.2 (Aosong Electronics Co., 2023a).

Tabel 4.2. Perbandingan Karakteristik Modul DHT11 dan DHT22

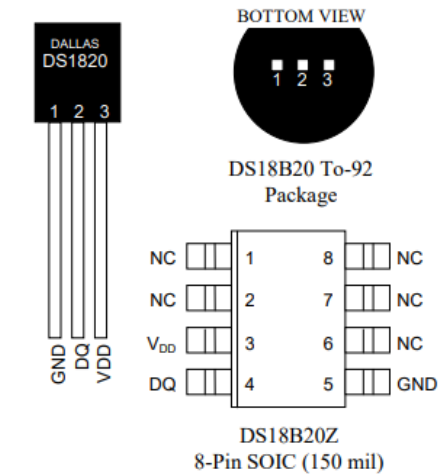
Fitur	DHT11	DHT22
Tegangan Kerja	3 to 5Vdc	3 to 5Vdc
Arus Maksimal	2.5mA max	2.5mA max
Humidity Range	20-80% / 5%	0-100% / 2-5%
Temperature Range	0-50°C / $\pm 2^\circ C$	-40 to 80°C / $\pm 0.5^\circ C$
Sampling Rate	1 Hz (reading every second)	0.5 Hz (reading every 2 seconds)
Advantage	Ultra low cost	More Accurate

Sumber: (lastminuteengineers, 2023), (Aosong Electronics Co., 2023b)



Gambar 4.3. Pinout Modul Sensor DHT11 dan DHT22
(Sumber : (Texas Instruments, 2017))

Modul DS18B20, merupakan Termometer Digital yang menyediakan pembacaan suhu 9 hingga 12-bit (dapat dikonfigurasi) yang menunjukkan suhu perangkat. Informasi dikirim ke/dari DS18B20 melalui antarmuka 1-Wire, sehingga hanya satu kabel yang dihubungkan dari mikroprosesor ke DS18B20. Akurasi dalam membaca, menulis, dan melakukan konversi suhu dapat diperoleh dari jalur data itu sendiri tanpa memerlukan eksternal sumber daya (Dallas Semiconductor, 2023).



PIN DESCRIPTION

GND - Ground
DQ - Data In/Out
V_{DD} - Power Supply Voltage
NC - No Connect

Gambar 4.4. Pinout Modul Sensor DS18B20
(Sumber : Dallas Semiconductor, 2023)

4.2.3 Desain dan Konfigurasi Sistem Sensor pada IoT

Desain Sistem Sensor pada IoT: Proses desain melibatkan pemilihan sensor yang sesuai dengan kebutuhan aplikasi, pemilihan protokol komunikasi yang efisien, dan integrasi sensor dengan platform IoT yang digunakan.

Konfigurasi Sistem Sensor pada IoT: Langkah-langkah konfigurasi mencakup kalibrasi sensor untuk akurasi pengukuran, pengaturan frekuensi pengukuran berdasarkan kebutuhan aplikasi, dan implementasi langkah-langkah keamanan data sensor (Sheltami et al., 2015).

4.3 Aktuator dalam IoT

Aktuator/Penggerak merupakan perangkat elektromekanik yang menghasilkan daya gerakan yang bertindak berdasarkan perintah yang diterima dari sistem IoT. Aktuator dapat melakukan tindakan fisik seperti mengaktifkan atau mematikan perangkat, menggerakkan mekanisme, mengubah suhu, atau mengontrol

keadaan lainnya di lingkungan fisik (Andaria *et al.*, 2023). Aktuator sendiri bisa juga didefinisikan sebagai komponen yang mengubah energi listrik menjadi mekanik/Gerakan (kelasrobot.com, 2014). Aktuator dalam IoT adalah perangkat yang merespons sinyal atau perintah dari sistem IoT untuk melakukan aksi fisik atau mengubah keadaan lingkungan.

4.3.1 Prinsip Kerja Aktuator pada IoT

Aktuator bekerja berdasarkan prinsip konversi energi. Mereka mengambil energi yang diberikan oleh sinyal kontrol atau sumber energi dan mengubahnya menjadi gerakan fisik. Prinsip kerja aktuator dapat bervariasi tergantung pada jenisnya. Berikut ini adalah beberapa prinsip kerja yang umum digunakan :

1. **Elektromagnetik** : Aktuator elektromagnetik menggunakan medan magnet yang dihasilkan oleh arus listrik untuk menghasilkan gerakan. Prinsip ini digunakan dalam Motor DC (permanent magnet, brushless, shunt dan series), Motor DC Servo, Motor DC Stepper, Ultrasonic Motor, Linear Motor, *Torque Motor*, Solenoid, *Relay*, dsb.) (Jaya, 2016).
2. **Hidraulis (berbasis bahan cair seperti oli)** : Aktuator hidraulis menggunakan fluida bertekanan, seperti minyak hidraulis, untuk menghasilkan gerakan linear atau putar. Tekanan hidraulis yang diberikan pada piston menghasilkan gaya yang mendorong gerakan aktuator.
3. **Pneumatik (perangkat kompresi berbasis udara atau gas nitrogen)** : Aktuator pneumatik menggunakan udara bertekanan untuk menghasilkan gerakan mekanik. Udara bertekanan mengalir ke dalam ruang yang diatur, menggerakkan piston dan menghasilkan gerakan yang diinginkan (Mukhtar *et al.*, 2023).

4.3.2 Jenis-Jenis penguatan Aktuator pada IoT

Berdasarkan jenis penguatannya, aktuator diklasifikasikan menjadi tiga kategori, yaitu aktuator listrik aktuator hidrolik, dan aktuator pneumatik (Taufiqurrachman, 2015) (Elga Aris Prastyo, 2022a).

Beberapa jenis aktuator umum dalam IoT meliputi:

1. Aktuator Motor/Elektrik: Digunakan untuk menggerakkan atau mengendalikan perangkat mekanis, berdasarkan listrik.
 - a. Motor Servo : Motor servo adalah motor yang mampu bekerja dua arah (CW dan CCW) dimana arah dan sudut pergerakan rotornya dapat dikendalikan hanya dengan memberikan pengaturan *duty cycle* sinyal PWM pada bagian pin kontrolnya. Motor Servo merupakan sebuah motor DC yang memiliki rangkaian control elektronik dan internal gear untuk mengendalikan pergerakan dan sudut angularnya. Motor servo adalah motor yang berputar lambat, dimana biasanya ditunjukkan oleh rate putarannya yang lambat, namun demikian memiliki torsi yang kuat karena internal gearnya (Jaya, 2016).



Gambar 4.5. Motor servo
(Sumber : Prastyo, 2022)

- b. Motor Stepper : Motor stepper mengubah pulsa listrik yang diberikan menjadi gerakan rotor discret (berlainan) yang disebut step (langkah). Satu derajat-per langkah motor memerlukan 360 pulsa untuk menggerakkan melewati satu putaran. Juga ada motor mikro step dengan ribuan langkah per putaran.



Gambar 4.6. Motor stepper
(Sumber : Elga Aris Prastyo, 2022)

- c. Motor DC (*Direct Current*) : jenis motor paling sederhana, yang memiliki dua kabel, yaitu catu daya (positif) dan Ground. Pemberian catu daya boleh dibolak-balik untuk memberikan efek arah putaran yang berbeda. Motor akan berputar terus selama catu daya diberikan dan berhenti ketika catu daya. Rangkaian di dalam Motor DC terdiri dari kumparan/lilitan konduktor. Setiap arus yang mengalir melalui sebuah konduktor yang akan menimbulkan medan magnet. Konduktor dibentuk menjadi sebuah loop sehingga ada dua bagian konduktor yang berada di dalam medan magnet pada saat yang sama (Prastyo, 2018).



Gambar 4.7. Motor DC
(Sumber : Prastyo, 2018)

2. Aktuator Pneumatik: Mengubah energi pneumatik menjadi gerakan fisik. *Pneumatic* berasal dari bahasa Yunani yang berarti udara atau angin. Definisi *pneumatic* merupakan salah

satu cabang ilmu fisika yang mempelajari fenomena udara yang dimampatkan (bertekanan) sehingga tekanan yang terjadi akan menghasilkan gaya sebagai penyebab gerak / aktuasi pada aktuator (Direktorat Pembinaan SMK, 2017).

- a. Aktuator Piston Pneumatik : merupakan jenis aktuator yang dapat bekerja dengan mengubah energi yang diciptakan oleh kompresi udara menjadi gerakan mekanis. Aktuator ini berisi piston yang dapat membantu menghasilkan tenaga motif dari udara untuk menjaga udara agar tetap tinggi, sehingga dapat memaksa diafragma untuk memutar atau memindahkan batang katup (Elga Aris Prastyo, 2022b).



Gambar 4.8. Aktuator Piston Pneumatik
(Sumber : (Elga Aris Prastyo, 2022b))

- b. Silinder pneumatik ganda aksi (*Double-acting pneumatic cylinder*): Ini adalah salah satu jenis aktuator pneumatik paling umum. Silinder ini memiliki dua saluran udara yang memungkinkannya untuk bergerak maju dan mundur ketika udara terkompresi dimasukkan atau dikeluarkan secara bergantian. Contoh penggunaannya termasuk pintu otomatis, mesin industri, dan peralatan handling material.
- c. Aktuator pneumatik rotary: Aktuator ini mengubah energi udara terkompresi menjadi gerakan rotasi. Mereka digunakan untuk menggerakkan katup putar, pengaturan posisi, atau mekanisme putar lainnya. Contoh

penggunaannya termasuk katup bola pneumatik pada sistem pengaturan aliran fluida.

- d. Kerucut pneumatik (*Pneumatic actuated valve*): Ini adalah aplikasi umum dari aktuator pneumatik di mana udara terkompresi digunakan untuk menggerakkan katup. Saat aktuator diberi tekanan, katup akan terbuka atau tertutup sesuai dengan kebutuhan dalam sistem perpipaan untuk mengontrol aliran fluida.
 - e. Robotik pneumatik: Di beberapa kasus, sistem robotika sederhana menggunakan aktuator pneumatik untuk menggerakkan bagian-bagian mekanis, seperti gripper untuk mengambil atau melepaskan objek, atau bahkan dalam aplikasi manipulasi sederhana.
3. Aktuator Hidrolik: perangkat yang menggunakan cairan hidrolik (biasanya minyak atau cairan hidrolik khusus) sebagai media untuk mentransfer energi dan menghasilkan gerakan linier atau rotasi. Mereka sering digunakan dalam aplikasi industri yang memerlukan kekuatan besar dan kemampuan untuk menghasilkan gerakan yang presisi. Aktuator hidrolik umumnya digunakan di mana aktuator pneumatik tidak memberikan kekuatan yang cukup atau di mana diperlukan kekuatan tinggi. Prinsip dasar dari aktuator hidrolik adalah menggunakan tekanan cairan hidrolik untuk menggerakkan piston atau silinder yang kemudian menghasilkan gerakan mekanis. Ketika tekanan diberikan pada cairan hidrolik, piston akan bergerak maju atau mundur, menggerakkan bagian mekanis yang terhubung dengannya.
- a. Silinder hidrolik (*Hydraulic cylinder*): Ini adalah jenis aktuator hidrolik paling umum. Silinder hidrolik terdiri dari tabung berisi piston yang dapat bergerak maju dan mundur. Ketika tekanan cairan hidrolik diberikan ke satu sisi piston, itu mendorong piston ke arah yang berlawanan, menghasilkan gerakan linier. Contoh penggunaannya termasuk mesin penggiling, mesin cetak, dan mesin konstruksi berat seperti alat berat.
 - b. Motor hidrolik (*Hydraulic motor*): Ini adalah aktuator hidrolik yang menghasilkan gerakan rotasi. Mereka sering

digunakan di kendaraan konstruksi, mesin pertanian, dan aplikasi industri lainnya yang memerlukan gerakan rotasi dengan kekuatan tinggi, seperti penggerak roda pada truk derek.

- c. Sistem hidrolik pada kendaraan (*Hydraulic systems in vehicles*): Sistem hidrolik digunakan dalam banyak kendaraan, terutama di sistem pengereman hidrolik pada mobil dan truk. Ketika pedal rem ditekan, tekanan hidrolik dihasilkan untuk menggerakkan kaliper rem, yang kemudian mendorong bantalan rem ke rotor untuk menghasilkan gaya pengereman.
- d. Alat-alat bantu hidrolik (*Hydraulic jacks and lifts*): Alat-alat bantu hidrolik digunakan untuk mengangkat beban berat, seperti kendaraan atau peralatan berat di bengkel atau gudang. Mereka bekerja dengan menerapkan tekanan hidrolik untuk mengangkat beban secara vertikal.

4.3.3 Desain dan Konfigurasi Sistem Aktuator pada IoT

Desain Sistem Aktuator pada IoT: Proses desain melibatkan pemilihan aktuator yang sesuai dengan kebutuhan aksi fisik yang diinginkan, serta integrasi aktuator dengan sistem kontrol yang digunakan dalam IoT.

Konfigurasi Sistem Aktuator pada IoT: Langkah-langkah konfigurasi mencakup pengaturan respons aktuator untuk mencapai hasil yang diinginkan, dan pemantauan kinerja aktuator secara berkala untuk memastikan kehandalan operasional (Mukhtar *et al.*, 2023)

DAFTAR PUSTAKA

- Andaria, A.C. *et al.* (2023) 'Alat Pakan Otomatis Berbasis IoT Pada Tambak Ikan Nila', *Jurnal Sistem Komputer Trinita*, 1(1), pp. 1–10. Available at: <https://jsk.trinita.ac.id/index.php/ait/article/view/24> (Accessed: 12 March 2024).
- Aosong Electronics Co., L. (2023a) *Digital-output relative humidity & temperature sensor/module*. Available at: <https://datasheetspdf.com/pdf-file/792211/Aosong/DHT22/1> (Accessed: 12 March 2024).
- Aosong Electronics Co., L. (2023b) *Humidity & Temperature sensor/module*. Available at: <https://datasheetspdf.com/pdf-file/785591/Aosong/DHT11/1> (Accessed: 12 March 2024).
- Dallas Semiconductor (2023) *DS18B20 Programmable Resolution 1-Wire Digital Thermometer*. Available at: www.dalsemi.com (Accessed: 12 March 2024).
- Direktorat Pembinaan SMK (2017) *Modul Pneumatik Dengan Aplikasinya*.
- Jaya, H. (2016) *Desain Dan Implementasi Sistem Robotika Berbasis Mikrokontroler*. Pertama. Edukasi Mitra Grafika.
- kelasrobot.com (2014) *Macam-Macam Actuator (Motor) Robot*, <https://kelasrobot.com/blog/2014/11/16/macam-macam-actuator-motor-robot/>.
- lastminuteengineers (2023) *Interfacing DHT11 and DHT22 Sensors with Arduino*, lastminuteengineers.com. Available at: <https://lastminuteengineers.com/dht11-dht22-arduino-tutorial/> (Accessed: 12 March 2024).
- Mukhtar, A. *et al.* (2023) *Sensor Dan Aktuator: Konsep Dasar Dan Aplikasi*. Pertama. Edited by A. Masruroh. Penerbit Widina Media Utama. Available at: www.freepik.com.
- Nugroho, A., Prathivi, R. and Daru, A.F. (2019) 'Analisa Metode Validasi Sensor Suhu Untuk Aplikasi Internet Of Things (Analysis Of Validation Temperature Sensor Method For The Internet Of Things Application)', *Pengembangan Rekayasa dan Teknologi*, 15(1). Available at: <http://journals.usm.ac.id/index.php/jprt/index>.

- Prastyo, E.A. (2018) *Motor DC / Dinamo DC*, <https://www.arduinoindonesia.id/>. Available at: <https://www.arduinoindonesia.id/2018/08/motor-dc-dinamo-dc.html> (Accessed: 6 May 2024).
- Prastyo, Elga Aris (2022a) 'Design of Steel Reheating Furnace Gas Actuator Control System Using Arduino UNO', *Journal Of Informatics And Telecommunication Engineering*, 6(1), pp. 49–59. Available at: <https://doi.org/10.31289/jite.v6i1.7002>.
- Prastyo, Elga Aris (2022b) *Pengertian dan Penjelasan tentang Aktuator*, <https://www.arduinoindonesia.id/>. Available at: <https://www.arduinoindonesia.id/2022/10/pengertian-dan-penjelasan-tentang-aktuator.html> (Accessed: 6 May 2024).
- Prastyo, Elga A. (2022) *Pengertian dan Prinsip Kerja Motor Servo*, <https://www.arduinoindonesia.id/>.
- Prastyo, Elga Aris (2022c) *Penjelasan tentang Motor Stepper*, <https://www.arduinoindonesia.id/>. Available at: <https://www.arduinoindonesia.id/2022/08/penjelasan-tentang-motor-stepper.html> (Accessed: 6 May 2024).
- Texas Instruments (2017) 'LM35 Precision Centigrade Temperature Sensors'. Available at: <https://www.ti.com/lit/ds/symlink/lm35.pdf> (Accessed: 12 March 2024).

BAB 5

KEAMANAN DAN PRIVASI DALAM IOT

Oleh Yendi Putra

5.1 Pendahuluan

Keamanan dan privasi dalam *Internet of Things* (IoT) merupakan isu yang sangat krusial dalam era digital saat ini. IoT merujuk pada jaringan perangkat yang saling terhubung melalui internet, memungkinkan pertukaran data secara *real-time*. Namun, seiring dengan pertumbuhan penggunaan IoT, muncul berbagai tantangan terkait keamanan dan privasi. Dalam konteks ini, penting untuk memahami bahwa setiap perangkat yang terhubung ke internet berpotensi menjadi titik masuk bagi ancaman keamanan. Berbagai studi menunjukkan bahwa kerentanan pada perangkat IoT dapat dieksploitasi untuk tujuan jahat, seperti pencurian data pribadi atau penyerangan sistem secara menyeluruh. Oleh karena itu, upaya untuk memperkuat keamanan dan privasi dalam IoT bukan hanya tanggung jawab teknolog dan pengembang perangkat, tetapi juga pengguna dan regulator yang harus bekerja sama untuk menciptakan ekosistem yang aman dan terpercaya.

Isu privasi dalam IoT juga tidak kalah pentingnya. Data yang dikumpulkan oleh perangkat IoT sering kali sangat personal dan sensitif, mencakup informasi seperti lokasi, kebiasaan pengguna, dan data kesehatan. (Matheus & Gunadi, 2023) Penanganan data ini harus mematuhi berbagai regulasi privasi yang ada, seperti *General Data Protection Regulation* (GDPR) di Eropa, yang menuntut adanya persetujuan eksplisit dari pengguna sebelum data mereka dapat dikumpulkan dan diproses. Meski demikian, masih banyak tantangan yang harus dihadapi untuk memastikan bahwa privasi pengguna tetap terlindungi. Salah satu tantangan terbesar adalah bagaimana memastikan transparansi dalam pengumpulan dan penggunaan data, sehingga pengguna dapat membuat keputusan yang sadar mengenai data mereka. (Laza & Karo Karo, 2023)

Inovasi teknologi dalam IoT juga membawa risiko baru yang memerlukan pendekatan keamanan yang lebih canggih. Misalnya, penggunaan kecerdasan buatan (AI) dan machine learning dalam perangkat IoT dapat meningkatkan efisiensi dan fungsi perangkat, tetapi juga membuka celah baru bagi serangan siber. Penelitian menunjukkan bahwa algoritma AI bisa dieksploitasi untuk membuat serangan yang lebih kompleks dan sulit dideteksi. Oleh karena itu, pengembangan solusi keamanan yang mampu mengantisipasi dan merespon ancaman ini sangat penting. Pendekatan yang komprehensif, termasuk penerapan enkripsi yang kuat, autentikasi multi-faktor, dan monitoring jaringan secara berkelanjutan merupakan beberapa langkah yang dapat diambil untuk meningkatkan keamanan IoT.

Peran edukasi dan kesadaran pengguna juga tidak bisa diabaikan dalam menjaga keamanan dan privasi dalam IoT. Pengguna sering kali menjadi target termudah bagi serangan siber karena kurangnya pemahaman mengenai praktik keamanan yang baik. Oleh karena itu, edukasi yang berkelanjutan mengenai pentingnya keamanan siber, cara mengenali ancaman potensial, dan langkah-langkah yang bisa diambil untuk melindungi diri sangat diperlukan. Program pelatihan dan kampanye kesadaran yang melibatkan berbagai pihak, termasuk pemerintah, perusahaan teknologi, dan organisasi masyarakat, dapat membantu meningkatkan kesadaran dan pemahaman mengenai isu ini. Dengan demikian, menciptakan budaya keamanan siber yang kuat dan berkelanjutan akan membantu dalam mengurangi risiko yang dihadapi dalam ekosistem IoT.

5.2 Definisi Keamanan dan Privasi dalam IoT

Keamanan dalam konteks IoT merujuk pada perlindungan perangkat dan jaringan dari serangan yang dapat mengkompromikan integritas, kerahasiaan, dan ketersediaan data yang dikumpulkan dan dikomunikasikan. Keamanan IoT mencakup berbagai aspek, termasuk enkripsi data, autentikasi pengguna, otorisasi akses, dan deteksi serta pencegahan serangan. Tanpa langkah-langkah keamanan yang memadai, perangkat IoT dapat menjadi target empuk bagi peretas, yang dapat mengeksploitasi

kerentanan untuk mencuri informasi, mengontrol perangkat dari jarak jauh, atau mengganggu operasi sistem.

Privasi dalam IoT berhubungan dengan perlindungan informasi pribadi yang dikumpulkan oleh perangkat IoT. Privasi mencakup bagaimana data dikumpulkan, disimpan, diproses, dan dibagikan. Dalam banyak kasus, perangkat IoT mengumpulkan data yang sangat pribadi, seperti lokasi pengguna, kebiasaan sehari-hari, data kesehatan, dan interaksi sosial. Oleh karena itu, penting untuk memastikan bahwa data ini dilindungi dari akses yang tidak sah dan hanya digunakan untuk tujuan yang sah dan sesuai dengan persetujuan pengguna. Keamanan dan privasi dalam IoT sering kali saling terkait, namun memiliki fokus yang berbeda. Keamanan lebih menekankan pada aspek teknis untuk mencegah akses yang tidak sah dan menjaga integritas sistem, sementara privasi lebih berfokus pada perlindungan hak-hak individu terkait data pribadi mereka. Keduanya sangat penting untuk memastikan bahwa adopsi IoT tidak menimbulkan risiko yang tidak diinginkan bagi pengguna.

Implementasi keamanan dan privasi dalam IoT bukanlah tugas yang mudah, mengingat keragaman perangkat, aplikasi, dan lingkungan operasional. Setiap jenis perangkat mungkin memiliki kebutuhan keamanan yang berbeda, tergantung pada fungsinya dan jenis data yang dikumpulkan. Oleh karena itu, pendekatan keamanan dan privasi harus bersifat holistik dan mencakup berbagai lapisan perlindungan.

5.3 Pentingnya Keamanan dan Privasi dalam IoT

Keamanan dan privasi dalam IoT adalah dua aspek yang sangat krusial mengingat dampak potensial dari pelanggaran yang mungkin terjadi. Keamanan yang buruk dapat menyebabkan berbagai ancaman, termasuk pencurian data, gangguan operasional, dan bahkan risiko fisik jika perangkat yang dikendalikan menjadi sasaran serangan. Misalnya, serangan pada perangkat medis dapat mengancam keselamatan pasien, sementara serangan pada sistem transportasi dapat menyebabkan kecelakaan dan kerugian ekonomi yang signifikan. Privasi juga menjadi perhatian utama karena data yang dikumpulkan oleh perangkat IoT sering kali bersifat pribadi dan sensitif. Pelanggaran privasi dapat mengakibatkan

penyalahgunaan data, seperti pencurian identitas, pemerasan, dan pelacakan aktivitas individu tanpa sepengetahuan atau persetujuan mereka. Hal ini dapat merusak kepercayaan pengguna terhadap teknologi IoT dan menghambat adopsi serta perkembangan lebih lanjut dari teknologi ini.

Selain itu, regulasi yang semakin ketat terkait perlindungan data pribadi, seperti General Data Protection Regulation (GDPR) di Uni Eropa, menuntut perusahaan untuk mengimplementasikan langkah-langkah keamanan dan privasi yang lebih ketat. Kegagalan untuk mematuhi regulasi ini dapat mengakibatkan denda yang besar dan kerugian reputasi yang signifikan bagi perusahaan. Oleh karena itu, memastikan keamanan dan privasi dalam IoT bukan hanya masalah teknis, tetapi juga kewajiban hukum dan etika. Pentingnya keamanan dan privasi dalam IoT juga tercermin dalam kebutuhan untuk mendidik dan meningkatkan kesadaran pengguna. Banyak pengguna mungkin tidak menyadari risiko yang terkait dengan penggunaan perangkat IoT atau cara melindungi diri mereka dari ancaman tersebut. Oleh karena itu, pendidikan dan kesadaran tentang praktik keamanan dan privasi yang baik sangat penting untuk melindungi pengguna dan memastikan bahwa mereka dapat menikmati manfaat dari IoT tanpa mengorbankan keamanan dan privasi mereka.

5.4 Jenis Kasus Serangan Pada IOT

Beberapa kasus keamanan IoT yang signifikan selama lima tahun terakhir diantaranya sebagai berikut:

Tabel 5.2. Jenis Serangan Pada IoT

No	Nama Serangan	Teknik Serangan	Target dan Dampak serangan
1	Mirai Botnet (2016)	Mirai adalah salah satu serangan malware terbesar yang menargetkan perangkat IoT pada tahun 2016. Malware ini menginfeksi	Mirai menargetkan berbagai perangkat IoT yang memiliki keamanan lemah. Beberapa jenis perangkat yang paling banyak

No	Nama Serangan	Teknik Serangan	Target dan Dampak serangan
		perangkat-perangkat seperti kamera keamanan, DVR, dan router, dan kemudian menggunakan perangkat-perangkat tersebut untuk melakukan serangan distribusi layanan (DDoS), menyebabkan gangguan besar pada layanan online. Teknik seranganya adalah (Affinito et al., 2023): 1. Pemindaian Jaringan: Mirai melakukan pemindaian secara terus-menerus terhadap alamat IP publik untuk menemukan perangkat IoT yang terhubung ke internet. 2. Eksploitasi Kredensial Default: Setelah menemukan perangkat IoT, Mirai mencoba	terinfeksi termasuk: 1. Kamera CCTV dan kamera IP. 2. Router rumah dan perangkat jaringan lainnya. 3. Perekam video digital (DVR). Dampak Serangan: 1. Gangguan Layanan Internet: Salah satu serangan paling terkenal yang dilancarkan oleh Mirai adalah serangan DDoS terhadap Dyn, sebuah perusahaan penyedia DNS, pada 21 Oktober 2016. Serangan ini mengakibatkan gangguan besar pada layanan internet di Amerika Serikat dan Eropa, mempengaruhi

No	Nama Serangan	Teknik Serangan	Target dan Dampak serangan
		login menggunakan daftar kredensial default atau mudah ditebak yang biasanya tidak diubah oleh pengguna. Perangkat yang berhasil diakses kemudian diinfeksi dengan malware Mirai. 3. Komunikasi dengan Server Command-and-Control (C2): Perangkat yang terinfeksi berkomunikasi dengan server C2 untuk menerima perintah dari pengendali botnet. Server ini mengkoordinasikan serangan yang dilancarkan oleh botnet. 4. Pelaksanaan Serangan DDoS: Setelah cukup banyak perangkat terinfeksi dan menjadi bagian	situs web besar seperti Twitter, GitHub, Reddit, Netflix, dan banyak lainnya. 2. Skala Serangan: Serangan DDoS yang dilancarkan oleh Mirai mencapai puncaknya dengan lalu lintas mencapai 1.1 terabit per detik (Tbps), menjadikannya salah satu serangan DDoS terbesar dalam sejarah pada waktu itu.

No	Nama Serangan	Teknik Serangan	Target dan Dampak serangan
		dari botnet, Mirai dapat melancarkan serangan Distributed Denial of Service (DDoS) dengan mengirimkan lalu lintas jaringan yang sangat besar ke target, menyebabkan overload pada server atau jaringan dan membuatnya tidak dapat diakses oleh pengguna sah.	
2.	Serangan BlueBorne (2017)	BlueBorne adalah serangan yang memanfaatkan kerentanan Bluetooth pada perangkat IoT, termasuk smartphone, speaker pintar, dan perangkat lain yang menggunakan teknologi Bluetooth. Serangan ini memungkinkan penyerang untuk mengambil alih perangkat tanpa	BlueBorne menargetkan berbagai perangkat dengan implementasi Bluetooth yang rentan, termasuk: 1. Smartphones: Ponsel pintar yang menjalankan Android, iOS, dan Windows Phone. 2. Komputer: PC dan laptop yang

No	Nama Serangan	Teknik Serangan	Target dan Dampak serangan
		interaksi pengguna, membahayakan keamanan data dan privasi pengguna 1. Eksploitasi Kerentanan Bluetooth: BlueBorne mengeksploitasi sejumlah kerentanan yang ada di tumpukan Bluetooth, termasuk dalam sistem operasi Android, iOS, Windows, dan Linux. Kerentanan ini memungkinkan penyerang untuk mengambil alih perangkat target tanpa memerlukan interaksi pengguna. 2. Tanpa Interaksi Pengguna: Salah satu fitur paling berbahaya dari BlueBorne adalah bahwa serangan ini tidak	menjalankan Windows dan Linux. 3. Perangkat IoT: Berbagai perangkat IoT yang menggunakan Bluetooth, seperti perangkat rumah pintar, speaker, headset, dan perangkat medis. Dampak Serangan: 1. Pengambilalihan Perangkat: Penyerang dapat memperoleh kontrol penuh atas perangkat yang terinfeksi, memungkinkan mereka untuk mencuri data, memasang malware, atau menggunakan perangkat sebagai titik awal untuk serangan lebih lanjut. 2. Penyebaran

No	Nama Serangan	Teknik Serangan	Target dan Dampak serangan
		memerlukan interaksi pengguna. Perangkat hanya perlu memiliki Bluetooth diaktifkan dan berada dalam jangkauan penyerang. 3. Eksekusi Kode Jarak Jauh: Penyerang dapat mengirimkan payload berbahaya melalui koneksi Bluetooth, yang dieksekusi di perangkat target. Ini memungkinkan pengambilalihan penuh perangkat, termasuk akses ke data pribadi, instalasi malware 4. Penyebaran Lokal: BlueBorne juga dapat menyebar dari satu perangkat yang terinfeksi ke perangkat lain	Malware: BlueBorne memiliki kemampuan untuk menyebar dari satu perangkat ke perangkat lain melalui koneksi Bluetooth, memungkinkan penyebaran malware secara cepat di lingkungan dengan banyak perangkat yang rentan.

No	Nama Serangan	Teknik Serangan	Target dan Dampak serangan
		yang rentan di sekitarnya melalui Bluetooth, membuatnya mirip dengan worm (Wang et al., 2023).	
3	Serangan Ripple20 (2020)	Ripple20 adalah serangkaian 19 kerentanan yang ditemukan oleh perusahaan keamanan JSOF dalam pustaka perangkat lunak Treck TCP/IP. Pustaka ini banyak digunakan dalam perangkat IoT dan sistem tertanam. Berikut adalah teknik yang digunakan dalam serangan Ripple20 (Ryan et al., 2024): 1. Eksploitasi Kerentanan TCP/IP: Kerentanan ini ditemukan dalam implementasi protokol jaringan TCP/IP yang	Target Serangan: Ripple20 mempengaruhi berbagai jenis perangkat yang menggunakan pustaka Treck TCP/IP, termasuk: 1. Perangkat IoT: Berbagai perangkat rumah pintar seperti kamera keamanan, termostat pintar, dan sistem pencahayaan. 2. Peralatan Medis: Alat kesehatan yang digunakan di rumah sakit dan fasilitas medis, seperti monitor pasien, pompa infus, dan perangkat diagnostik.

No	Nama Serangan	Teknik Serangan	Target dan Dampak serangan
		digunakan untuk mengelola komunikasi data di berbagai perangkat. Kerentanan ini melibatkan berbagai masalah seperti buffer overflow, integer overflow, improper handling of IP fragments, dan lain-lain 2. Remote Code Execution (RCE): Beberapa kerentanan dalam Ripple20 memungkinkan eksekusi kode jarak jauh. Penyerang dapat mengirimkan paket jaringan yang dirancang khusus untuk memicu kerentanan ini dan menjalankan kode berbahaya di perangkat target.	3. Perangkat Industri: Sistem kontrol industri dan perangkat SCADA yang digunakan di pabrik, utilitas, dan infrastruktur kritis lainnya. 4. Perangkat Jaringan: Router, switch, dan perangkat jaringan lainnya yang menggunakan pustaka Treck TCP/IP untuk komunikasi (Zaman & Zaman, 2015). Dampak Serangan: 1. Pengambilalihan Perangkat: Eksploitasi kerentanan RCE memungkinkan penyerang untuk mengambil alih perangkat yang rentan, memberikan mereka kontrol penuh atas

No	Nama Serangan	Teknik Serangan	Target dan Dampak serangan
		3. Denial of Service (DoS): Beberapa kerentanan memungkinkan penyerang untuk menyebabkan perangkat yang rentan crash atau menjadi tidak responsif, mengakibatkan gangguan layanan 4. Data Exfiltration: Memungkinkan penyerang untuk mengakses data sensitif yang disimpan atau diproses oleh perangkat yang rentan, memungkinkan pencurian data atau informasi pribadi.	perangkat tersebut. 2. Kemampuan untuk mengakses data sensitif: Memungkinkan pencurian informasi pribadi, data medis, atau informasi bisnis penting, yang dapat digunakan untuk tujuan jahat atau dijual di pasar gelap.

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.

5.5 Ancaman Keamanan dalam IoT

Internet of Things (IoT) telah membawa kemudahan dan kenyamanan dalam kehidupan sehari-hari, tetapi juga memperkenalkan berbagai ancaman keamanan yang kompleks. Untuk memahami bagaimana ancaman ini dapat memengaruhi sistem IoT, penting untuk memahami beberapa bentuk serangan yang paling umum terjadi. Serangan siber pada perangkat IoT merupakan ancaman yang semakin meningkat karena pesatnya pertumbuhan perangkat yang terhubung ke internet. Serangan semacam ini dimungkinkan karena banyaknya perangkat IoT yang memiliki keamanan yang lemah atau tidak memadai. Penyerang dapat memanfaatkan kerentanan ini untuk mengambil alih kontrol perangkat, mencuri data, atau merusak sistem. Untuk lebih memahami serangan siber pada perangkat IoT (Butarbutar, 2023).

5.5.1 Eksploitasi Kerentanan Perangkat Lunak dan Perangkat Keras

Perangkat IoT sering kali menggunakan perangkat lunak yang tidak terbaru atau tidak memiliki pembaruan keamanan yang rutin. Hal ini membuat mereka rentan terhadap serangan yang memanfaatkan celah keamanan yang telah diketahui atau ditemukan. Penyerang dapat mengeksploitasi kerentanan ini untuk mendapatkan akses ke perangkat, mengubah pengaturan, atau bahkan menginstal malware.

Contoh:

Sebuah kamera keamanan yang menggunakan perangkat lunak yang tidak terbaru dapat menjadi sasaran serangan siber jika ada celah keamanan yang diketahui di versi perangkat lunak tersebut. Penyerang dapat memanfaatkan celah ini untuk mendapatkan akses ke kamera dan menggunakannya untuk memantau aktivitas di dalam rumah tanpa sepengetahuan penghuni.

5.5.2 Serangan Melalui Jaringan

Serangan siber pada perangkat IoT juga dapat terjadi melalui jaringan, di mana penyerang mengeksploitasi kelemahan dalam jaringan rumah atau kantor untuk mendapatkan akses ke perangkat

IoT yang terhubung. Ini dapat dilakukan dengan menerobos router atau firewall yang tidak terlindungi, mengambil alih kontrol perangkat yang terhubung ke jaringan, atau memanfaatkan kredensial yang lemah(Munawar et al., 2020).

Contoh:

Seorang penyerang yang telah mendapatkan akses ke jaringan Wi-Fi rumah atau kantor dapat menggunakan teknik serangan "*man-in-the-middle*" untuk memata-matai lalu lintas data yang melewati jaringan. Dengan memata-matai lalu lintas ini, penyerang dapat mencuri informasi sensitif seperti kata sandi atau data keuangan.

5.5.3 Serangan Fisik

Serangan siber pada perangkat IoT juga dapat terjadi secara fisik, di mana penyerang mendapatkan akses fisik ke perangkat untuk memanipulasi atau merusaknya. Ini dapat dilakukan dengan membobol perangkat, mengganti perangkat kerasnya, atau memasang perangkat tambahan yang tidak diotorisasi.

Contoh:

Seorang penyerang dapat mencuri perangkat IoT dari rumah atau kantor target dan membongkar perangkat tersebut untuk mendapatkan akses ke komponen internalnya. Dengan memiliki akses fisik ke perangkat, penyerang dapat memanipulasi atau merusak perangkat tersebut sesuai keinginannya.

5.6 Privasi dalam IoT

Privasi merupakan aspek yang sangat penting dalam penggunaan teknologi *Internet of Things* (IoT), mengingat bahwa perangkat IoT sering kali mengumpulkan dan memproses data pribadi pengguna secara terus-menerus. Namun, penggunaan perangkat IoT juga membawa risiko terhadap privasi.



Gambar 5.1. Ilustrasi IOT
Sumber: techtarget-com

Pengguna jika tidak dilakukan dengan hati-hati. Dalam konteks ini, penting untuk memahami risiko privasi yang terkait dengan penggunaan IoT, bagaimana data sensitif dikumpulkan dan diproses, serta upaya-upaya untuk melindungi privasi pengguna dan mematuhi regulasi yang berlaku.

5.6.1 Risiko Privasi dalam Penggunaan IoT

Data sensitif dalam konteks *Internet of Things* (IoT) mengacu pada informasi yang bersifat pribadi dan sensitif yang dikumpulkan oleh perangkat IoT tentang pengguna. Perangkat IoT sering kali mengumpulkan beragam data yang meliputi informasi tentang kesehatan, lokasi, aktivitas harian, dan preferensi pengguna. Misalnya, perangkat kesehatan pintar dapat mencatat detak jantung, tingkat aktivitas, atau pola tidur seseorang, sedangkan perangkat rumah pintar seperti kamera keamanan dapat merekam aktivitas di dalam rumah. Data-data ini memiliki nilai sensitif yang tinggi karena mereka memberikan gambaran yang sangat rinci tentang kehidupan dan kebiasaan pengguna.

Dengan adanya pengumpulan data sensitif oleh perangkat IoT, timbullah kekhawatiran terkait privasi dan keamanan data.

Data sensitif seperti informasi kesehatan atau aktivitas harian dapat digunakan untuk membuat profil pengguna yang sangat rinci, yang dapat menimbulkan risiko privasi yang signifikan jika jatuh ke tangan yang salah. Selain itu, data sensitif juga rentan terhadap penyalahgunaan, pencurian, atau akses yang tidak sah oleh pihak yang tidak berwenang. Penting untuk memahami bahwa perlindungan data sensitif dalam IoT merupakan tanggung jawab bersama antara pengembang perangkat IoT, penyedia layanan, dan pengguna. Pengembang perangkat IoT harus menerapkan langkah-langkah keamanan yang kuat untuk melindungi data sensitif pengguna, seperti enkripsi data, otentikasi yang kuat, dan pembaruan keamanan teratur. Di sisi pengguna, penting untuk menyadari risiko yang terkait dengan penggunaan perangkat IoT dan mengambil langkah-langkah untuk melindungi privasi mereka, seperti memilih perangkat yang memiliki keamanan yang kuat, mengelola izin akses, dan mengaktifkan pengaturan privasi yang disediakan oleh perangkat tersebut.

Melalui kerjasama antara pengembang, penyedia layanan, dan pengguna, data sensitif dalam IoT dapat dilindungi dengan lebih baik, sehingga memastikan bahwa privasi pengguna tetap terjaga dalam lingkungan yang semakin terhubung secara digital. Dengan memperhatikan risiko-risiko yang terkait dengan data sensitif, langkah-langkah proaktif dapat diambil untuk mengurangi kemungkinan penyalahgunaan atau pelanggaran privasi yang tidak diinginkan.

Risiko privasi dalam penggunaan *Internet of Things* (IoT) menjadi semakin signifikan seiring dengan adopsi yang semakin luas dari perangkat-perangkat yang terhubung ke internet. Perangkat IoT sering kali mengumpulkan data pribadi pengguna tanpa pengetahuan atau persetujuan mereka, yang dapat mengancam privasi individu. Risiko-risiko ini dapat diuraikan dengan lebih detail sebagai berikut:

1. Pengumpulan Data Tanpa Izin:

Salah satu risiko utama dalam penggunaan IoT adalah pengumpulan data tanpa izin atau pengetahuan pengguna. Perangkat IoT sering kali terhubung secara terus-menerus ke internet, dan mereka dapat secara otomatis

- mengumpulkan data tentang aktivitas pengguna, preferensi, dan kebiasaan mereka tanpa sepengetahuan mereka. Ini mencakup data seperti lokasi, aktivitas online, dan informasi kesehatan yang sensitif.
2. **Penggunaan Data yang Tidak Diketahui:**
Data yang dikumpulkan oleh perangkat IoT sering kali digunakan untuk tujuan yang tidak diketahui oleh pengguna. Perusahaan yang mengembangkan atau mengoperasikan perangkat IoT dapat menggunakan data ini untuk profil pengguna, menyediakan iklan yang disesuaikan, atau bahkan menjual data kepada pihak ketiga tanpa persetujuan pengguna.
 3. **Pembobolan Keamanan Data:**
Perangkat IoT rentan terhadap pembobolan keamanan yang dapat mengakibatkan akses tidak sah ke data pengguna. Kelemahan dalam perangkat lunak atau kurangnya pembaruan keamanan dapat dimanfaatkan oleh penyerang untuk mendapatkan akses ke data pribadi pengguna yang disimpan di dalam perangkat IoT.
 4. **Ketergantungan pada Layanan Cloud:** B
anyak perangkat IoT menyimpan data pengguna di server cloud, yang meningkatkan risiko privasi karena data tersebut dapat diakses dari jarak jauh. Jika server cloud tersebut diretas atau kompromi, data sensitif pengguna dapat dicuri atau diakses oleh pihak yang tidak sah.
 5. **Kehilangan Kontrol atas Data:**
Penggunaan perangkat IoT dapat menyebabkan pengguna kehilangan kontrol atas data pribadi mereka. Seiring dengan pertumbuhan ekosistem IoT yang semakin rumit, sulit bagi pengguna untuk mengetahui atau mengontrol bagaimana data mereka dikumpulkan, disimpan, dan digunakan oleh perusahaan yang mengembangkan atau menggunakan perangkat IoT.

Risiko-risiko ini menunjukkan bahwa privasi pengguna dalam konteks IoT perlu diperhatikan dengan serius, dan langkah-langkah perlu diambil untuk memastikan bahwa data pribadi

pengguna dilindungi dengan baik. Ini termasuk menerapkan praktik keamanan yang kuat, memberikan transparansi kepada pengguna tentang praktik pengumpulan dan pengolahan data, serta memberikan pengguna kontrol yang lebih besar atas data mereka. Dengan langkah-langkah ini, risiko-risiko privasi dalam penggunaan IoT dapat dikelola dengan lebih efektif.

5.6.2 Data Sensitif dalam IoT

Data sensitif dalam konteks *Internet of Things* (IoT) mengacu pada informasi yang bersifat pribadi dan sensitif yang dikumpulkan oleh perangkat IoT tentang pengguna. Perangkat IoT sering kali mengumpulkan beragam data yang meliputi informasi tentang kesehatan, lokasi, aktivitas harian, dan preferensi pengguna. Misalnya, perangkat kesehatan pintar dapat mencatat detak jantung, tingkat aktivitas, atau pola tidur seseorang, sedangkan perangkat rumah pintar seperti kamera keamanan dapat merekam aktivitas di dalam rumah. Data-data ini memiliki nilai sensitif yang tinggi karena mereka memberikan gambaran yang sangat rinci tentang kehidupan dan kebiasaan pengguna (Haque et al., 2023).

Dengan adanya pengumpulan data sensitif oleh perangkat IoT, timbulah kekhawatiran terkait privasi dan keamanan data. Data sensitif seperti informasi kesehatan atau aktivitas harian dapat digunakan untuk membuat profil pengguna yang sangat rinci, yang dapat menimbulkan risiko privasi yang signifikan jika jatuh ke tangan yang salah. Selain itu, data sensitif juga rentan terhadap penyalahgunaan, pencurian, atau akses yang tidak sah oleh pihak yang tidak berwenang.

Penting untuk memahami bahwa perlindungan data sensitif dalam IoT merupakan tanggung jawab bersama antara pengembang perangkat IoT, penyedia layanan, dan pengguna. Pengembang perangkat IoT harus menerapkan langkah-langkah keamanan yang kuat untuk melindungi data sensitif pengguna, seperti enkripsi data, otentikasi yang kuat, dan pembaruan keamanan teratur. Di sisi pengguna, penting untuk menyadari risiko yang terkait dengan penggunaan perangkat IoT dan mengambil langkah-langkah untuk melindungi privasi mereka, seperti memilih perangkat yang memiliki keamanan yang kuat, mengelola izin akses, dan

mengaktifkan pengaturan privasi yang disediakan oleh perangkat tersebut.

Melalui kerjasama antara pengembang, penyedia layanan, dan pengguna, data sensitif dalam IoT dapat dilindungi dengan lebih baik, sehingga memastikan bahwa privasi pengguna tetap terjaga dalam lingkungan yang semakin terhubung secara digital. Dengan memperhatikan risiko-risiko yang terkait dengan data sensitif, langkah-langkah proaktif dapat diambil untuk mengurangi kemungkinan penyalahgunaan atau pelanggaran privasi yang tidak diinginkan.

5.6.3 Pengumpulan dan Pengolahan Data

Pengumpulan dan pengolahan data dalam konteks Internet of Things (IoT) merupakan proses penting yang melibatkan pengambilan, penyimpanan, analisis, dan penggunaan data yang dikumpulkan oleh perangkat IoT. Perangkat IoT secara terus-menerus mengumpulkan berbagai jenis data tentang pengguna, termasuk informasi tentang perilaku, preferensi, lokasi, dan lingkungan sekitarnya. Data ini kemudian disimpan di server atau cloud untuk dianalisis dan digunakan dalam berbagai aplikasi, seperti meningkatkan pengalaman pengguna, mengoptimalkan kinerja perangkat, atau memberikan layanan yang disesuaikan.

Setelah data dikumpulkan, langkah berikutnya adalah pengolahan data, di mana data tersebut dianalisis dan diolah untuk mendapatkan wawasan yang berharga. Analisis data dalam konteks IoT dapat mencakup penggunaan teknik-teknik seperti machine learning atau big data analytics untuk mengidentifikasi pola atau tren yang relevan dari data yang dikumpulkan. Data yang telah diproses kemudian dapat digunakan untuk membuat keputusan yang lebih baik, memperbaiki kinerja sistem, atau menyediakan layanan yang lebih personal kepada pengguna.

Penting untuk dicatat bahwa pengumpulan dan pengolahan data dalam IoT harus dilakukan dengan hati-hati dan sesuai dengan persyaratan privasi yang berlaku. Perusahaan yang mengembangkan atau mengoperasikan perangkat IoT memiliki tanggung jawab untuk memastikan bahwa data dikumpulkan dan diproses dengan cara yang aman dan sesuai dengan persyaratan

privasi pengguna. Ini termasuk memberikan informasi yang jelas kepada pengguna tentang jenis data yang dikumpulkan, tujuan pengumpulan data, serta hak-hak pengguna terkait data mereka, sesuai dengan regulasi yang berlaku seperti GDPR di Uni Eropa. Dengan memperhatikan kebutuhan privasi pengguna dan mematuhi regulasi yang berlaku, pengumpulan dan pengolahan data dalam IoT dapat dilakukan dengan etis dan bertanggung jawab.

5.6.4 Privasi Pengguna dan Kepatuhan Regulasi

Privasi pengguna dan kepatuhan terhadap regulasi merupakan aspek penting dalam ekosistem *Internet of Things* (IoT) yang berkembang pesat. Dengan semakin banyaknya perangkat yang terhubung ke internet dan mengumpulkan data pengguna, perlindungan privasi menjadi semakin penting. Regulasi seperti *General Data Protection Regulation* (GDPR) di Uni Eropa menetapkan standar yang ketat terkait dengan pengumpulan, pengolahan, dan penyimpanan data pribadi pengguna (Diamantopoulou et al., 2022). Hal ini mendorong perusahaan yang mengembangkan atau menggunakan perangkat IoT untuk mematuhi persyaratan privasi yang ketat dan melindungi data pengguna dengan cermat.

Pentingnya privasi pengguna tidak hanya berasal dari kepatuhan terhadap regulasi, tetapi juga dari tanggung jawab etis dan kepedulian terhadap keamanan data. Perusahaan yang mengembangkan atau menggunakan perangkat IoT harus mengambil langkah-langkah proaktif untuk melindungi privasi pengguna, termasuk menerapkan keamanan data yang kuat, memberikan kontrol yang lebih besar kepada pengguna atas data mereka, dan meningkatkan kesadaran tentang risiko privasi dalam penggunaan IoT.

Langkah-langkah konkret yang dapat diambil untuk memastikan privasi pengguna dan kepatuhan terhadap regulasi meliputi pengembangan kebijakan privasi yang jelas dan transparan, pelaksanaan sistem otentikasi yang kuat, dan penyediaan mekanisme untuk mengizinkan pengguna untuk mengontrol data mereka. Selain itu, perusahaan juga harus secara teratur memantau dan mengevaluasi kepatuhan mereka terhadap

regulasi yang berlaku serta memperbarui kebijakan dan praktik mereka sesuai dengan perkembangan teknologi dan hukum.

Dengan memperhatikan privasi pengguna dan mematuhi regulasi yang berlaku, perusahaan dapat membangun kepercayaan dengan pengguna mereka dan memastikan bahwa data pribadi pengguna diolah dengan cara yang etis dan bertanggung jawab. Ini bukan hanya keharusan hukum, tetapi juga merupakan elemen penting dari integritas dan reputasi perusahaan di era yang semakin terhubung secara digital.

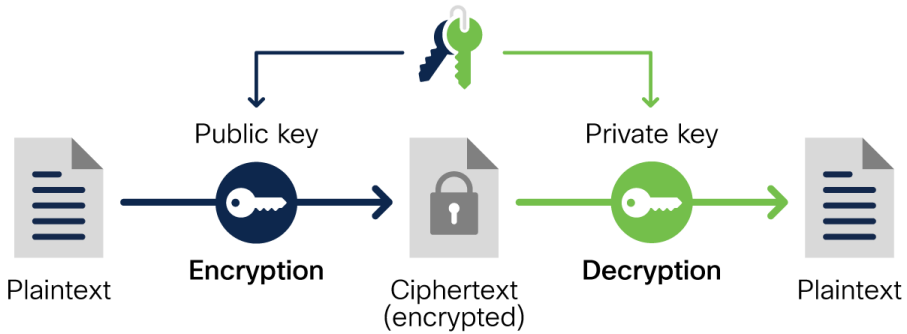
5.7 Teknologi Keamanan Untuk IoT

Internet of Things (IoT) telah membawa transformasi dalam berbagai aspek kehidupan, tetapi dengan pertumbuhan ekosistem IoT yang cepat, keamanan menjadi perhatian utama. Teknologi keamanan untuk IoT dirancang untuk melindungi perangkat IoT dan data yang dikirim dan diterima olehnya dari ancaman yang berpotensi merusak. Berikut adalah penjelasan detail tentang empat teknologi keamanan utama untuk IoT beserta implementasinya:

5.7.1 Enkripsi dan Keamanan Data

Enkripsi dan keamanan data merupakan aspek penting dalam melindungi informasi sensitif dari akses yang tidak sah atau penyalahgunaan. Enkripsi adalah proses mengubah teks biasa menjadi teks terenkripsi menggunakan algoritma tertentu sehingga hanya pihak yang memiliki kunci enkripsi yang tepat yang dapat membaca atau mendekripsi data tersebut.

Asymmetric encryption



Gambar 5.1. Proses Enkripsi Asymmetric
Sumber: cisco.com

Rumus Enkripsi

Enkripsi dapat diwakili secara umum dengan rumus matematika sebagai berikut:

$C = Ek(M)$ Di mana:

C adalah teks terenkripsi.

Ek adalah fungsi enkripsi dengan kunci k

M adalah teks biasa yang akan dienkripsi.

Beberapa algoritma enkripsi yang umum digunakan adalah:

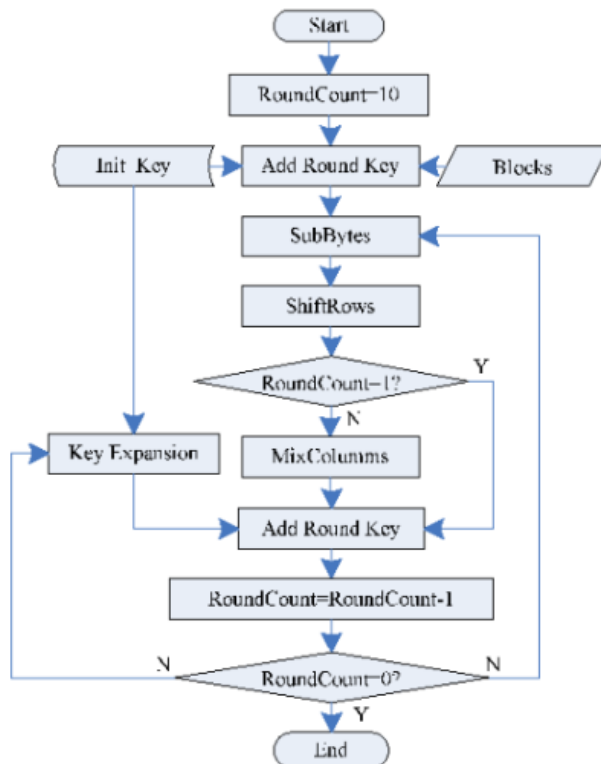
A. Advanced Encryption Standard (AES):

AES dikembangkan oleh dua kriptografer Vincent Rijmen dan Joan Daemen, AES diadopsi sebagai standar enkripsi oleh *National Institute of Standards and Technology* (NIST) pada tahun 2001. AES dipilih melalui proses kompetisi terbuka yang dimulai pada tahun 1997, AES merupakan salah satu algoritma enkripsi simetris yang paling umum digunakan. Ini menggunakan blok ukuran tetap 128-bit dan kunci enkripsi yang dapat berukuran 128, 192, atau 256 bit (Putra et al., 2021).
Karakteristik Utama

1. **Blok Enkripsi:** AES adalah cipher blok yang bekerja dengan blok data berukuran tetap sebesar 128 bit.

2. **Ukuran Kunci:** AES mendukung tiga panjang kunci yang berbeda, yaitu 128 bit, 192 bit, dan 256 bit. nama versi ini adalah AES-128, AES-192, dan AES-256.
3. **Struktur:** AES menggunakan struktur yang dikenal sebagai "substitution-permutation network" (SPN) dan terdiri dari beberapa putaran (rounds) enkripsi. Jumlah putaran bervariasi tergantung pada panjang kunci:
 1. 10 putaran untuk kunci 128 bit
 2. 12 putaran untuk kunci 192 bit
 3. 14 putaran untuk kunci 256 bit

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



Gambar 5.2. 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).

Contoh Aplikasi AES di IoT

1. Smart Home: Perangkat seperti kamera keamanan, thermostat, dan kunci pintu pintar menggunakan AES untuk mengamankan komunikasi antara perangkat dan server cloud.
2. Kesehatan: Alat kesehatan yang terhubung, seperti monitor glukosa dan perangkat pelacak kebugaran, menggunakan AES untuk melindungi data pribadi dan medis pengguna.
3. Industri: Sensor dan aktuator dalam sistem otomasi industri menggunakan AES untuk mengamankan data operasional dan kontrol.

Keuntungan Penggunaan AES di IoT

1. **Keamanan Tinggi:** AES menyediakan tingkat keamanan yang tinggi dengan panjang kunci yang memadai.
2. **Kinerja Efisien:** AES dapat diimplementasikan dengan efisien dalam perangkat keras dan perangkat lunak, menjadikannya cocok untuk perangkat IoT dengan sumber daya terbatas.
3. **Fleksibilitas:** Mendukung berbagai mode operasi dan panjang kunci, memungkinkan adaptasi sesuai kebutuhan spesifik perangkat dan aplikasi IoT.

B. RSA (*Rivest-Shamir-Adleman*):

Algoritma RSA (*Rivest-Shamir-Adleman*) adalah salah satu algoritma kriptografi kunci publik yang paling terkenal dan banyak digunakan. RSA digunakan untuk enkripsi dan dekripsi data serta tanda tangan digital. RSA didasarkan pada kesulitan faktorisasi bilangan besar. Keamanan RSA terletak pada kenyataan bahwa sangat sulit untuk memfaktorkan produk dari dua bilangan prima besar.

Langkah-langkah Algoritma RSA

1. Pembuatan Kunci

- a. Pilih dua bilangan prima besar, p dan q :
 - Bilangan prima ini harus dipilih secara acak dan aman.
- b. Hitung n sebagai hasil perkalian p dan q : $n=p \times q$
 - n digunakan sebagai modulus dalam kunci publik dan kunci privat.
- c. Hitung 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 .
- d. Pilih bilangan bulat e (eksponen publik):
 - e harus memenuhi $1 < e < \phi(n)$ dan $\text{gcd}(e, \phi(n)) = 1$.
- e. Hitung d (eksponen privat):
 - d adalah invers modular dari e modulo $\phi(n)$, yaitu: $d \times e \equiv 1 \pmod{\phi(n)}$

2. Kunci Publik dan Privat:

- Kunci Publik: (e, n)
- Kunci Privat: (d, n)

3. Enkripsi:

- Pesan plaintext M (harus dalam bentuk bilangan bulat yang lebih kecil dari n): $C = M^e \pmod{n}$ adalah ciphertext hasil enkripsi.

4. Dekripsi:

- Ciphertext C : $M = C^d \pmod{n}$
- M adalah plaintext yang berhasil didekripsi.

5.7.2 Perlindungan Data

Keamanan data melibatkan upaya untuk melindungi data dari akses yang tidak sah atau perubahan yang tidak sah. Enkripsi adalah salah satu metode utama dalam melindungi data. Dengan mengenkripsi data, bahkan jika data tersebut diretas atau diakses oleh pihak yang tidak berwenang, data yang terbaca tetap dalam bentuk terenkripsi yang tidak dapat dimengerti tanpa kunci yang tepat.

5.7.3 Penggunaan Kunci

Penting untuk menjaga keamanan kunci enkripsi. Kunci yang lemah atau mudah ditebak dapat mengorbankan keamanan data. Oleh karena itu, kunci harus dihasilkan secara acak dan memiliki panjang yang cukup untuk menghindari serangan bruteforce. Selain itu, rotasi kunci secara teratur juga merupakan praktik yang baik untuk menjaga keamanan data dalam jangka panjang.

5.7.4 Implementasi pada IoT

Dalam konteks *Internet of Things* (IoT), enkripsi dan keamanan data sangat penting karena perangkat IoT sering kali mengirimkan data sensitif melalui jaringan yang rentan terhadap serangan. Implementasi enkripsi pada IoT dapat dilakukan dengan menggunakan protokol enkripsi seperti TLS (*Transport Layer Security*) atau protokol enkripsi khusus yang dirancang untuk IoT seperti MQTT-TLS. Penggunaan enkripsi ini memastikan bahwa data yang dikirim antar perangkat IoT atau ke server cloud dilindungi secara aman dari akses yang tidak sah.

Dengan demikian, enkripsi dan keamanan data merupakan langkah yang penting dalam menjaga privasi dan keamanan data dalam ekosistem IoT yang semakin terhubung. Dengan menerapkan algoritma enkripsi yang kuat dan mengelola kunci dengan baik, kita dapat memastikan bahwa data sensitif tetap aman dan terlindungi dari ancaman yang berpotensi merusak.

5.8 Autentikasi dan Otorisasi

Autentikasi dan otorisasi adalah dua konsep yang kunci dalam menjaga keamanan sistem, termasuk dalam konteks Internet of Things (IoT). Keduanya bekerja sama untuk memastikan bahwa hanya pengguna yang sah yang memiliki akses terhadap sumber daya atau informasi yang diinginkan, dan hanya dapat melakukan tindakan yang diizinkan. Berikut adalah penjelasan lebih rinci tentang autentikasi dan otorisasi:



Gambar 5.3. Autentikasi pada IoT

Sumber: strongdm.com

5.8.1 Autentikasi

Autentikasi adalah proses memverifikasi identitas seseorang atau perangkat untuk memastikan bahwa mereka adalah entitas yang mereka klaim.

Metode Autentikasi

1. **Username dan Password:** Metode autentikasi yang paling umum adalah menggunakan kombinasi username dan password.
2. **Token:** Pengguna diberikan token unik yang harus mereka berikan sebagai bukti identitas mereka.
3. **Biometrik:** Identifikasi berdasarkan ciri-ciri fisik unik, seperti sidik jari atau pemindaian wajah.

Implementasi pada IoT

Dalam IoT, autentikasi digunakan untuk memverifikasi identitas perangkat yang terhubung ke jaringan. Setiap perangkat diberikan kredensial autentikasi yang unik, seperti token atau sertifikat digital. Protokol autentikasi yang umum digunakan dalam IoT termasuk OAuth, JWT (JSON Web Token), dan X.509 certificates. Dengan autentikasi yang kuat, kita dapat memastikan bahwa hanya perangkat yang sah yang memiliki akses ke jaringan IoT dan layanan terkait.

5.8.1 Otorisasi

Otorisasi adalah proses memberikan hak akses atau izin kepada pengguna atau perangkat setelah mereka berhasil melewati proses autentikasi.

1. **Hak Akses:** Mengidentifikasi jenis akses apa yang diizinkan untuk pengguna atau perangkat tertentu.
2. **Kontrol Akses:** Memastikan bahwa pengguna atau perangkat hanya memiliki akses ke sumber daya atau layanan yang sesuai dengan hak akses mereka.
3. **Manajemen Hak Akses:** Mengelola hak akses secara dinamis sesuai dengan perubahan dalam lingkungan atau peraturan.

Implementasi pada IoT

Dalam konteks IoT, otorisasi digunakan untuk mengendalikan akses perangkat terhadap data dan layanan. Setelah perangkat atau pengguna terotentikasi, sistem otorisasi akan menentukan apa yang dapat mereka lakukan dalam jaringan IoT. Misalnya, perangkat yang terotentikasi sebagai sensor mungkin memiliki hak akses untuk mengirimkan data sensor, tetapi tidak untuk mengubah pengaturan perangkat lain. Implementasi yang tepat dari otorisasi memastikan bahwa hanya tindakan yang diizinkan yang dapat dilakukan dalam ekosistem IoT, yang membantu melindungi data dan mencegah penyalahgunaan.

Dengan memahami dan menerapkan autentikasi dan otorisasi dengan benar dalam sistem IoT, kita dapat memastikan bahwa hanya entitas yang sah yang memiliki akses terhadap data

dan sumber daya, serta dapat melakukan tindakan yang sesuai dengan wewenang mereka. Ini adalah langkah kunci dalam menjaga keamanan dan integritas dalam ekosistem yang semakin terhubung secara digital.

5.9 Keamanan Jaringan dan Komunikasi

Keamanan jaringan dan komunikasi adalah aspek penting dalam ekosistem *Internet of Things* (IoT) karena perangkat IoT sering kali terhubung ke jaringan yang rentan terhadap serangan dari pihak yang tidak berwenang. Perlindungan jaringan dan komunikasi dalam konteks IoT melibatkan upaya untuk mencegah akses yang tidak sah ke perangkat dan data, serta memastikan bahwa data yang dikirim antara perangkat IoT dan server atau antar perangkat tetap aman dan terjamin. Berikut adalah penjelasan lebih rinci tentang keamanan jaringan dan komunikasi dalam konteks IoT:

5.9.1 Keamanan Jaringan

Serangan terhadap jaringan IoT dapat mencakup serangan man-in-the-middle, di mana penyerang mencoba untuk menyusup ke dalam komunikasi antara perangkat dan server, serta serangan *denial-of-service* (DDoS), di mana penyerang berusaha mengganggu ketersediaan jaringan dengan membanjiri jaringan dengan lalu lintas yang tidak sah. (Suryono, 2022)

Solusi

Penggunaan firewall dan deteksi intrusi adalah beberapa solusi yang umum digunakan untuk melindungi jaringan IoT dari serangan. Firewall dapat mengontrol akses ke jaringan dan memblokir lalu lintas yang mencurigakan, sementara deteksi intrusi dapat mendeteksi aktivitas yang mencurigakan atau serangan yang sedang berlangsung.

5.9.2 Keamanan Komunikasi

Data yang dikirim antara perangkat IoT dan server atau antar perangkat dapat rentan terhadap intersepsi atau modifikasi oleh pihak yang tidak berwenang. Ancaman ini dapat

mengakibatkan pencurian data atau manipulasi data yang dapat mengganggu integritas data.

Solusi

Penerapan protokol enkripsi yang kuat adalah kunci untuk menjaga keamanan komunikasi dalam IoT. Protokol seperti *Transport Layer Security* (TLS) atau protokol enkripsi khusus yang dirancang untuk IoT, seperti MQTT-TLS, dapat digunakan untuk mengamankan data saat berpindah melalui jaringan. Dengan menggunakan enkripsi, data yang dikirim antara perangkat IoT dan server atau antar perangkat tetap terlindungi dan tidak dapat dimengerti oleh pihak yang tidak berwenang (Taherdoost, 2023).

5.9.3 Penggunaan Protokol Keamanan

Dalam implementasi praktis, perangkat IoT dapat menggunakan protokol keamanan seperti HTTPS (HTTP Secure) untuk komunikasi dengan server, yang menggunakan enkripsi SSL/TLS untuk melindungi data. Selain itu, protokol seperti IPSec (*Internet Protocol Security*) dapat digunakan untuk mengamankan komunikasi antara perangkat IoT dalam jaringan lokal.

5.9.4 Pemantauan dan Pembaruan

Pemantauan lalu lintas jaringan dan pembaruan perangkat lunak secara teratur juga penting untuk menjaga keamanan jaringan dan komunikasi dalam IoT. Pemantauan dapat membantu mendeteksi aktivitas yang mencurigakan atau serangan yang sedang berlangsung, sementara pembaruan perangkat lunak dapat memperbaiki kerentanan keamanan yang baru ditemukan dan menjaga perangkat tetap aman dari serangan.

Dengan memperhatikan keamanan jaringan dan komunikasi dalam desain dan implementasi sistem IoT, kita dapat memastikan bahwa data yang dikirim antara perangkat IoT dan server atau antar perangkat tetap terlindungi dan aman dari ancaman yang berpotensi merusak. Ini adalah langkah kunci dalam menjaga keamanan dan integritas dalam ekosistem IoT yang semakin terhubung secara digital.

5.9.5 Strategi dan Praktik Keamanan dalam IoT

Strategi dan Praktik Keamanan dalam IoT" merujuk pada pendekatan dan tindakan yang diperlukan untuk menjaga keamanan dalam lingkungan *Internet of Things* (IoT). IoT melibatkan konektivitas yang luas antara perangkat fisik dan digital, yang meningkatkan kompleksitas dan risiko keamanan yang terkait. Berikut adalah beberapa poin yang dibahas dalam konteks ini

5.9.6 Mengidentifikasi dan Mengelola Risiko pada IoT

Mengidentifikasi dan mengelola risiko dalam IoT adalah langkah penting dalam menjaga keamanan sistem. Berikut adalah beberapa tahapan yang dapat diambil dalam proses ini:

1. **Identifikasi Risiko:** Langkah pertama adalah mengidentifikasi potensi risiko yang terkait dengan implementasi IoT. Ini bisa meliputi risiko keamanan seperti serangan peretasan, risiko privasi seperti pencurian data pribadi, dan risiko operasional seperti kegagalan perangkat yang dapat menyebabkan gangguan layanan. Identifikasi risiko ini dapat melibatkan analisis keamanan informasi, tinjauan arsitektur sistem, dan penggunaan teknik seperti threat modeling (Arini et al., 2022).
2. **Penilaian Risiko:** Setelah risiko diidentifikasi, langkah selanjutnya adalah mengevaluasi dampak potensial dari setiap risiko dan kemungkinan terjadinya. Ini membantu dalam menentukan prioritas dan fokus untuk tindakan mitigasi. Penilaian risiko dapat menggunakan metode seperti analisis risiko kuantitatif atau kualitatif.
3. **Pengembangan Strategi Mitigasi:** Berdasarkan penilaian risiko, langkah selanjutnya adalah mengembangkan strategi untuk mengurangi atau menghilangkan risiko tersebut. Strategi mitigasi dapat mencakup penerapan kontrol keamanan tambahan, perubahan desain sistem, atau kebijakan operasional baru. Penting untuk memilih strategi yang sesuai dengan tingkat risiko dan kebutuhan bisnis.
4. **Implementasi Tindakan Mitigasi:** Setelah strategi mitigasi ditetapkan, langkah berikutnya adalah menerapkan tindakan mitigasi yang dipilih. Ini mungkin melibatkan

penerapan perangkat lunak keamanan tambahan, pelatihan staf, atau perubahan prosedur operasional. Implementasi harus dilakukan dengan hati-hati untuk memastikan bahwa solusi keamanan tidak mengganggu fungsionalitas atau kinerja sistem.

5. **Pemantauan dan Tinjauan:** Langkah terakhir adalah memantau efektivitas tindakan mitigasi yang diimplementasikan dan melakukan tinjauan berkala terhadap risiko. Ini memastikan bahwa sistem tetap dilindungi terhadap ancaman yang berkembang dan bahwa strategi mitigasi tetap relevan. Pemantauan juga memungkinkan untuk mendeteksi dan merespons dengan cepat terhadap ancaman baru atau kegagalan sistem (Nurain et al., 2024).

Dengan mengidentifikasi dan mengelola risiko secara proaktif, organisasi dapat mengurangi kemungkinan kejadian yang tidak diinginkan dan melindungi infrastruktur IoT mereka dari ancaman keamanan.

5.9.7 Pembaruan dan Manajemen Perangkat

Pembaruan dan manajemen perangkat sangat penting untuk menjaga keamanan perangkat IoT dari kerentanan keamanan yang baru ditemukan. Perangkat IoT sering kali memiliki kerentanan keamanan yang dapat dieksploitasi oleh penyerang, dan oleh karena itu, pembaruan perangkat lunak secara teratur menjadi kunci untuk menjaga keamanan perangkat. Implementasi pembaruan perangkat pada IoT melibatkan penggunaan mekanisme pembaruan otomatis atau pengelolaan perangkat yang terpusat untuk memastikan bahwa semua perangkat IoT menerima pembaruan keamanan yang diperlukan secara tepat waktu.

5.9.8 Framework Keamanan IOT

Framework Keamanan IoT adalah kerangka kerja yang menyediakan panduan dan struktur untuk merencanakan, menerapkan, dan mengelola keamanan dalam lingkungan *Internet of Things* (IoT). Framework ini membantu organisasi dalam

memahami aspek-aspek keamanan yang relevan dan mengidentifikasi langkah-langkah yang diperlukan untuk melindungi infrastruktur dan data mereka. Berikut adalah komponen-komponen umum dari sebuah Framework Keamanan IoT:

1. **Identifikasi Risiko:** Framework keamanan IoT harus mencakup langkah-langkah untuk mengidentifikasi dan mengevaluasi risiko yang terkait dengan implementasi IoT. Ini dapat meliputi ancaman keamanan seperti serangan peretasan, risiko privasi seperti pencurian data pribadi, dan risiko operasional seperti kegagalan perangkat.
2. **Otentikasi dan Otorisasi:** Komponen penting dari keamanan IoT adalah memastikan bahwa hanya perangkat dan pengguna yang sah yang dapat mengakses sistem dan data. Framework harus menyediakan panduan untuk menerapkan mekanisme otentikasi yang kuat dan sistem otorisasi yang memadai.
3. **Enkripsi Data:** Data yang ditransmisikan dan disimpan dalam lingkungan IoT harus dienkripsi untuk melindungi kerahasiaan dan integritasnya. Framework harus menyediakan pedoman untuk memilih dan menerapkan algoritma enkripsi yang sesuai dengan tingkat keamanan yang dibutuhkan.
4. **Pemantauan dan Pemulihan:** Framework harus mencakup strategi untuk memantau aktivitas sistem secara terus-menerus dan mendeteksi potensi ancaman keamanan. Selain itu, itu harus memberikan panduan untuk merespons dengan cepat terhadap insiden keamanan dan mengembalikan sistem ke keadaan yang aman.
5. **Manajemen Identitas dan Akses:** Framework keamanan IoT harus mencakup strategi untuk mengelola identitas pengguna dan perangkat, serta mengontrol akses mereka ke sumber daya sistem. Ini dapat mencakup manajemen kredensial, kontrol akses berbasis peran, dan pembaruan otomatis untuk hak akses.
6. **Pembaruan dan Pemeliharaan:** Karena ancaman keamanan terus berkembang, Framework harus mencakup strategi

untuk memastikan bahwa perangkat dan perangkat lunak IoT tetap diperbarui dengan patch keamanan terbaru. Ini juga harus menyediakan panduan untuk pemeliharaan rutin dan pengelolaan rentang hidup perangkat.

7. **Kepatuhan dan Kebijakan:** Framework keamanan IoT harus sesuai dengan persyaratan peraturan dan standar keamanan yang relevan. Ini juga harus memberikan panduan untuk mengembangkan kebijakan keamanan internal yang memenuhi kebutuhan bisnis dan kebutuhan kepatuhan.

Dengan mengadopsi Framework Keamanan IoT yang tepat, organisasi dapat mengurangi risiko keamanan, melindungi data sensitif, dan mempertahankan kepercayaan pengguna dalam ekosistem IoT mereka.

Best Practices untuk Desain dan Implementasi Keamanan IoT

Adalah seperangkat pedoman dan tindakan yang direkomendasikan untuk memastikan bahwa sistem IoT tetap aman dari berbagai ancaman keamanan. Berikut adalah beberapa praktik terbaik yang dapat diikuti dalam desain dan implementasi keamanan IoT:

1. **Pemikiran Keamanan Dari Awal (*Security by Design*):** Integrasikan keamanan dalam setiap tahap siklus hidup pengembangan IoT, dari perencanaan hingga pensiun. Ini termasuk menentukan kebutuhan keamanan, memilih teknologi yang aman, dan merancang arsitektur yang tahan terhadap serangan.
2. **Penggunaan Protokol Komunikasi Aman:** Gunakan protokol komunikasi yang aman seperti HTTPS untuk mengenkripsi data yang ditransmisikan antara perangkat IoT dan platform backend. Protokol ini membantu melindungi data dari pengintai dan serangan Man-in-the-Middle.
3. **Otentikasi yang Kuat:** Pastikan bahwa setiap perangkat IoT diotentikasi secara unik sebelum diizinkan mengakses sistem atau data. Ini dapat dilakukan melalui metode

otentikasi seperti kredensial, sertifikat digital, atau kunci API.

4. **Enkripsi Data:** Enkripsi data pada perangkat, selama transmisi, dan saat disimpan di server. Ini memastikan bahwa data sensitif tidak dapat diakses oleh pihak yang tidak berwenang bahkan jika dicuri atau disadap.
5. **Pembaruan Perangkat Lunak Teratur:** Pastikan bahwa semua perangkat IoT diperbarui secara teratur dengan patch keamanan dan pembaruan perangkat lunak terbaru. Ini membantu memperbaiki kerentanan yang diketahui dan memastikan bahwa perangkat tetap dilindungi dari serangan baru.
6. **Pemantauan Keamanan:** Implementasikan sistem pemantauan keamanan untuk mendeteksi aktivitas mencurigakan atau serangan potensial pada perangkat IoT. Ini dapat meliputi pemantauan lalu lintas jaringan, analisis perilaku, dan pemberitahuan keamanan.
7. **Pemisahan Jaringan:** Gunakan segmentasi jaringan untuk memisahkan perangkat IoT dari jaringan lain, seperti jaringan kantor atau rumah. Ini membantu mencegah penyebaran serangan dan melindungi sistem yang lebih sensitif.
8. **Pelatihan Pengguna:** Berikan pelatihan keamanan kepada pengguna akhir untuk meningkatkan kesadaran mereka tentang risiko keamanan dan praktik terbaik yang harus diikuti. Ini termasuk memperkuat kata sandi, mengenali tanda-tanda serangan, dan melaporkan insiden keamanan.
9. **Pemulihan Bencana:** Siapkan rencana pemulihan bencana untuk mengatasi insiden keamanan yang parah atau kegagalan sistem. Ini termasuk cadangan data yang teratur, prosedur pemulihan, dan rencana kontinuitas bisnis.
10. **Kepatuhan dan Kebijakan:** Pastikan bahwa desain dan implementasi keamanan IoT mematuhi persyaratan peraturan dan standar keamanan yang relevan. Ini termasuk GDPR untuk privasi data, ISO 27001 untuk manajemen keamanan informasi, dan standar industri lainnya.

5.10 Regulasi dan Standar Keamanan IoT

Regulasi dan standar keamanan memainkan peran penting dalam menentukan kerangka kerja yang memandu pengembangan, implementasi, dan penggunaan *Internet of Things* (IoT). Dalam konteks ini, regulasi mengacu pada aturan dan peraturan yang ditetapkan oleh pemerintah atau badan pengatur untuk mengatur keamanan IoT, sedangkan standar adalah pedoman teknis yang dikeluarkan oleh badan standarisasi industri atau kelompok-kelompok yang berkaitan dengan teknologi.

5.10.1 Regulasi Global

Beberapa regulasi global yang berkaitan dengan keamanan IoT meliputi:

1. *General Data Protection Regulation* (GDPR): Regulasi Uni Eropa ini mengatur perlindungan data pribadi pengguna dan menetapkan persyaratan yang ketat untuk pengumpulan, pengolahan, dan penyimpanan data.
2. *California Consumer Privacy Act* (CCPA): Undang-undang ini di California, AS, memberikan hak kepada konsumen untuk mengetahui, mengendalikan, dan menghapus informasi pribadi yang dikumpulkan oleh perusahaan.
3. *Cybersecurity Law of the People's Republic of China*: Regulasi ini mengatur perlindungan data pribadi, keamanan jaringan, dan kewajiban perusahaan dalam melindungi data pengguna di Tiongkok.

5.10.2 Regulasi Lokal

Selain regulasi global, banyak negara dan yurisdiksi memiliki regulasi lokal yang mengatur keamanan IoT sesuai dengan kebutuhan dan tantangan yang spesifik di wilayah mereka. Beberapa standar industri yang diterapkan dalam konteks keamanan IoT meliputi:

1. **ISO/IEC 27001**: Standar internasional yang mengatur sistem manajemen keamanan informasi (ISMS) untuk memastikan keamanan informasi dalam sebuah organisasi.



Gambar 5.5. Standar Keamanan ISO/IEC 27001

Sumber: izinkanusa.id

2. **NIST *Cybersecurity Framework*:** Framework yang dikeluarkan oleh National Institute of Standards and Technology (NIST) AS, memberikan panduan tentang cara merancang, mengimplementasikan, dan meningkatkan keamanan dalam infrastruktur IT dan IoT.
3. **IoT Security Foundation (IoTSF):** Organisasi non-profit yang mengembangkan panduan dan sertifikasi keamanan untuk perangkat IoT.

5.11 Dampak Regulasi pada Pengembangan dan Implementasi IoT

Regulasi keamanan dapat memiliki dampak besar pada pengembangan produk IoT. Perusahaan harus memastikan bahwa produk mereka mematuhi persyaratan keamanan yang ditetapkan oleh regulasi untuk memastikan kepatuhan dan mencegah sanksi. Regulasi juga mempengaruhi cara implementasi dan penggunaan teknologi IoT. Organisasi harus memperhatikan persyaratan keamanan yang ditetapkan oleh regulasi saat menerapkan solusi IoT dan memastikan bahwa data pengguna dilindungi dengan benar.

Meskipun regulasi dapat memberikan tantangan tambahan, juga dapat mendorong inovasi keamanan dan memperkuat kepercayaan konsumen. Peraturan yang ketat tentang keamanan data dapat membantu membangun kepercayaan konsumen dalam teknologi IoT, yang pada gilirannya dapat mendorong pertumbuhan pasar yang lebih besar. Regulasi dan standar keamanan berperan penting dalam membentuk kerangka kerja untuk pengembangan, implementasi, dan penggunaan *Internet of Things*. Dengan mematuhi regulasi dan mengikuti standar yang relevan, perusahaan dapat memastikan bahwa solusi IoT mereka aman, andal, dan mematuhi standar etika dan privasi yang diperlukan dalam lingkungan digital yang semakin terhubung.

5.12 Masa Depan Keamanan dan Privasi dalam IoT

Keamanan dan privasi dalam *Internet of Things* (IoT) adalah bidang yang terus berkembang dan akan terus mengalami perubahan seiring dengan kemajuan teknologi dan dinamika pasar. Berikut adalah beberapa aspek kunci yang perlu dipertimbangkan dalam memahami masa depan keamanan dan privasi dalam IoT:

5.12.1 Tren dan Inovasi Teknologi Keamanan IoT

Tren dan inovasi dalam teknologi keamanan IoT terus berkembang sejalan dengan peningkatan kompleksitas infrastruktur IoT dan meningkatnya ancaman siber. Berikut ini adalah beberapa tren dan inovasi yang penting dalam konteks keamanan IoT:

- 1. Peningkatan Keamanan Perangkat**

Tren utama adalah peningkatan keamanan perangkat IoT itu sendiri. Hal ini mencakup penggunaan chip keamanan yang terintegrasi secara langsung dengan perangkat, yang dapat memberikan tingkat keamanan yang lebih tinggi daripada solusi perangkat lunak saja. Chip keamanan dapat menyediakan fitur-fitur seperti penyimpanan kunci enkripsi yang aman, proteksi perangkat keras terhadap serangan fisik, dan mekanisme autentikasi yang lebih kuat (Gangolli et al., 2022).

- 2. Keamanan Berbasis Identitas dan Akses**

Keamanan berbasis identitas dan akses menjadi semakin relevan dalam konteks IoT. Solusi autentikasi yang lebih canggih seperti biometrik (seperti sidik jari atau pemindaian wajah) semakin banyak digunakan untuk mengesahkan identitas pengguna atau perangkat. Ini membantu memastikan bahwa hanya entitas yang sah yang memiliki akses ke perangkat dan data IoT.

3. **Penggunaan Kecerdasan Buatan (AI) dan Analisis Data**
Penggunaan kecerdasan buatan (AI) dan analisis data menjadi tren penting dalam meningkatkan keamanan IoT. AI dapat digunakan untuk mendeteksi pola dan anomali yang tidak biasa dalam perilaku perangkat atau lalu lintas jaringan, yang dapat menjadi tanda serangan atau intrusi. Dengan menggunakan teknik pembelajaran mesin, sistem keamanan IoT dapat menjadi lebih adaptif dan responsif terhadap ancaman yang muncul.
4. **Penggunaan Teknologi Blockchain untuk Keamanan**
Blockchain juga menjanjikan untuk memberikan kontribusi besar terhadap keamanan IoT. Dengan menggunakan teknologi blockchain, catatan transaksi dan interaksi antar perangkat IoT dapat dipertahankan secara terdesentralisasi, aman, dan tidak dapat dimanipulasi. Ini membantu memastikan integritas data dan transparansi dalam lingkungan IoT.

5.12.3 Tantangan dan Peluang di Masa Depan IOT

Tantangan dan peluang di masa depan *Internet of Things* (IoT) menggambarkan dinamika kompleks yang dihadapi oleh industri dan pengguna saat teknologi ini terus berkembang. Berikut adalah beberapa tantangan dan peluang utama, serta contoh konkret yang mencerminkan setiap aspek tersebut:

1. **Tantangan:**

a. **Keamanan dan Privasi:**

- **Tantangan:** Masalah keamanan dan privasi menjadi perhatian utama dalam IoT karena perangkat yang terhubung secara luas meningkatkan permukaan serangan potensial.

Pelanggaran privasi data dan serangan siber menjadi ancaman nyata.

- **Contoh:** Serangan Mirai pada tahun 2016 adalah contoh nyata dari bagaimana botnet IoT dapat dimanfaatkan untuk meluncurkan serangan DDoS massal, mengganggu layanan Internet di seluruh dunia.

b. Skala dan Interoperabilitas:

- **Tantangan:** Skala infrastruktur IoT yang semakin besar dan keragaman perangkat yang terhubung menciptakan tantangan dalam mengelola dan mengkoordinasikan lingkungan yang kompleks.
- **Contoh:** Kesulitan dalam menciptakan standar dan protokol yang dapat diterima secara luas oleh semua perangkat IoT, sehingga menghambat interoperabilitas antarperangkat.

c. Daya Tahan dan Ketersediaan:

- **Tantangan:** Perangkat IoT seringkali harus beroperasi dalam lingkungan yang keras dan rentan terhadap gangguan. Ketersediaan sinyal, daya tahan perangkat, dan konektivitas menjadi perhatian penting.
- **Contoh:** Sensor lingkungan yang terpasang di daerah terpencil harus mampu bertahan dari kondisi cuaca ekstrim dan gangguan jaringan untuk memberikan data yang akurat secara konsisten.

2. Peluang:

a. Inovasi Teknologi:

- **Peluang:** Perkembangan teknologi seperti kecerdasan buatan, blockchain, dan komputasi edge membuka peluang baru untuk meningkatkan fungsionalitas dan keamanan dalam IoT (Nahdi & Dhika, 2021).
- **Contoh:** Penggunaan kecerdasan buatan untuk menganalisis data sensor dan mendeteksi pola anomali dapat membantu dalam mendeteksi

serangan siber dan meningkatkan keamanan sistem secara keseluruhan.

b. Penyebaran IoT di Industri:

- **Peluang:** Adopsi IoT semakin meluas di berbagai sektor industri, termasuk manufaktur, pertanian, kesehatan, dan energi. Ini membuka peluang untuk meningkatkan efisiensi operasional dan mengoptimalkan kinerja bisnis.
- **Contoh:** Penggunaan IoT dalam manufaktur untuk memonitor mesin dan proses produksi secara real-time dapat mengurangi downtime, meningkatkan produktivitas, dan mengurangi biaya perawatan.

c. Data dan Analitik:

- **Peluang:** IoT menghasilkan jumlah data yang besar dan beragam. Menganalisis data ini dengan bijaksana dapat menghasilkan wawasan berharga yang dapat digunakan untuk meningkatkan pengambilan keputusan dan memberikan layanan yang lebih baik kepada pengguna.
- **Contoh:** Dalam pertanian, sensor IoT dapat mengumpulkan data cuaca, tanah, dan tanaman yang dapat digunakan untuk memprediksi hasil panen, mengelola irigasi, dan meningkatkan efisiensi penggunaan sumber daya.

Memahami tantangan dan peluang di masa depan IoT membantu kita untuk merancang solusi yang lebih baik, mengatasi kendala, dan memanfaatkan potensi teknologi ini secara maksimal untuk menciptakan nilai tambah bagi masyarakat dan industri.

DAFTAR PUSTAKA

- Affinito, A., Zinno, S., Stanco, G., Botta, A., & Ventre, G. (2023). The evolution of Mirai botnet scans over a six-year period. *Journal of Information Security and Applications*, 79(October), 103629. <https://doi.org/10.1016/j.jisa.2023.103629>
- 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)
- Arini, A., Rozy, N. F., & Malik Matin, I. M. (2022). Uji Kerentanan Smart Home Menggunakan Metode Square Untuk Mendukung Smart Campus. *Cyber Security Dan Forensik Digital*, 4(2), 87–95. <https://doi.org/10.14421/csecurity.2021.4.2.3355>
- Butarbutar, R. (2023). Kejahatan Siber Terhadap Individu: Jenis, Analisis, Dan Perkembangannya. *Technology and Economics Law Journal*, 2(2), 299–317.
- Diamantopoulou, V., Lambrinoudakis, C., King, J., & Gritzalis, S. (2022). EU GDPR: Toward a Regulatory Initiative for Deploying a Private Digital Era. In *Modern Socio-Technical Perspectives on Privacy*. https://doi.org/10.1007/978-3-030-82786-1_18
- Gangolli, A., Mahmoud, Q. H., & Azim, A. (2022). A Systematic Review of Fault Injection Attacks on IoT Systems. *Electronics (Switzerland)*, 11(13). <https://doi.org/10.3390/electronics11132023>
- Haque, S., El-Moussa, F., Komninou, N., & Muttukrishnan, R. (2023). A Systematic Review of Data-Driven Attack Detection Trends in IoT. *Sensors*, 23(16), 1–29. <https://doi.org/10.3390/s23167191>
- Laza, J. M., & Karo Karo, R. (2023). Perlindungan Hukum Terhadap Artificial Intelligence Dalam Aspek Penyalahgunaan

- Deepfake Technology Pada Perspektif UU PDP dan GDPR [Legal Protection of Artificial Intelligence in Misusage of Deepfake Technology in the Perspective of PDP Law and GDPR]. *Lex Prospicit*, 1(2), 136.
<https://doi.org/10.19166/lp.v1i2.7386>
- Matheus, J., & Gunadi, A. (2023). Pembentukan Lembaga Pengawas Perlindungan Data Pribadi Di Era Ekonomi Digital : Kajian Perbandingan Dengan KPPU. *Justisi*, 10(1), 20–35.
<https://doi.org/10.33506/jurnaljustisi.v10i1.2757>
- Munawar, Z., Kom, M., & Putri, N. I. (2020). Keamanan Jaringan Komputer Pada Era Big Data. *Jurnal Sistem Informasi-J-SIKA*, 02(01), 14–20.
- Nahdi, F., & Dhika, H. (2021). Analisis Dampak Internet of Things (IoT) Pada Perkembangan Teknologi di Masa Yang Akan Datang. *INTEGER: Journal of Information Technology*, 6(1), 33–40. <https://doi.org/10.31284/j.integer.2021.v6i1.1423>
- Nurain, A., Gultom, R. A. G., & Indrajit, R. E. (2024). Manajemen Ketahanan Risiko Siber pada Internet of Things dan Cyber Physical System. *Journal on Education*, 06(02), 13271–13281.
<https://jonedu.org/index.php/joe/article/view/5179>
- Putra, Y., Yuhandri, Y., & Sumijan, S. (2021). Meningkatkan Keamanan Web Menggunakan Algoritma Advanced Encryption Standard (AES) terhadap Seragan Cross Site Scripting. *Jurnal Sistim Informasi Dan Teknologi*.
<https://doi.org/10.37034/jsisfotek.v3i2.44>
- Ryan, M. K., Rozier, K. Y., Ryan, M. K., & Rozier, K. Y. (2024). *A Survey and Analysis of Recent IoT Device Vulnerabilities A Survey and Analysis of Recent IoT Device Vulnerabilities*.
- Suryono, D. (2022). Analisis Keamanan Jaringan Hardware Trojan Pada IoT. *JATISI (Jurnal Teknik Informatika Dan Sistem Informasi)*, 9(4), 3529–3537.
<https://doi.org/10.35957/jatisi.v9i4.2845>
- Taherdoost, H. (2023). Security and Internet of Things: Benefits, Challenges, and Future Perspectives. *Electronics (Switzerland)*, 12(8), 1–22.
<https://doi.org/10.3390/electronics12081901>

- Wang, S., Chou, H. H., Izemski, A., Dinu, A., Vräjitoru, E. S., Toth, Z., & Boşcoianu, M. (2023). *Market in Medical Devices of Blockchain-Based IoT and Recent Cyberattacks*. 11(2), 39–44.
- Zaman, S., & Zaman, S. A. (2015). *Internet of Things (IoT) data protection and security concerns-Review*. <https://www.researchgate.net/publication/373439194>

BAB 6

PENANGANAN BIG DATA PADA INTERNET OF THINGS (IOT)

Oleh Kusnaeni

6.1 Pengertian Big Data

Big data merupakan kumpulan data dalam jumlah besar dan bersifat kompleks sehingga sulit dianalisis menggunakan metode konvensional. Big data memiliki beberapa karakteristik yang sering disebut dengan 5V yaitu *Volume, Variety, Velocity, Veracity, Value*.



Gambar 6.1. Karakteristik Big Data

(Sumber : <https://medium.com/@heni.muthiautami/pemanfaatan-dan-peluang-big-data-dalam-kehidupan-sehari-hari-974259b91de9>)

6.2 Karakteristik Big Data

Suatu data dikatakan big data jika memiliki karakteristik big data 5V yaitu *volume, variety, velocity, veracity, value*. karakteristik tersebut mencirikan bahwa big data memiliki kompleksitas dalam hal dimensi data yang besar, variasi data yang beragam, kecepatan

data yang terus bertambah, keandalan, kualitas dan keakuratan data. Serta nilai ekonomis dan strategis yang dapat diperoleh dari analisis data (Safar Dwi Kurniawan *et al.*, 2024).

6.2.1 Volume

Volume merupakan karakteristik dari big data yang paling umum didapatkan. *Volume* data merujuk kepada dimensi data yang berukuran besar yang dihasilkan atau dikumpulkan oleh sistem atau organisasi. Dimensi data dalam konteks big data terbilang sulit diselesaikan menggunakan metode tradisional contoh dari data dimensi besar yaitu:

1. Data media sosial
 - a. Postingan di media sosial seperti Facebook, Twitter, Instagram, dan platform media sosial lainnya menghasilkan data dalam jumlah besar setiap hari. Data ini dapat berupa teks, gambar, video, dan informasi lainnya tentang pengguna dan aktivitas pengguna.
 - b. Interaksi di media sosial contohnya Like, komentar, dan share adalah contoh interaksi di media sosial yang menghasilkan data tentang bagaimana pengguna berinteraksi di media sosial yang menghasilkan data tentang bagaimana pengguna berinteraksi dengan konten atau sama lain.
2. Data Transaksi
 - a. Transaksi keuangan seperti transaksi kartu kredit, transfer bank, dan pembelian online adalah contoh transaksi keuangan yang menghasilkan data tentang kebiasaan belanja dan pola keuangan individu dan bisnis.
 - b. Data ritel seperti Transaksi di toko, pembelian online, dan program loyalitas menghasilkan data tentang kebiasaan belanja dan preferensi konsumen.
3. Data Sensor
 - a. *Internet of Things* (IoT) adalah Perangkat IoT seperti *smart home devices*, *wearable devices*, dan sensor kendaraan menghasilkan data tentang bagaimana orang hidup, bekerja, dan bepergian.

- b. Sensor lingkungan adalah sensor yang dipasang di kota, hutan, dan laut mengumpulkan data tentang kualitas udara, polusi, dan kondisi cuaca.
- 4. Data Sains
 - a. Data genomik adalah data tentang DNA individu, yang dapat digunakan untuk penelitian medis dan pengembangan obat.
 - b. Data astronomi adalah data tentang bintang, galaksi, dan objek luar angkasa lainnya, yang dapat digunakan untuk penelitian ilmiah dan memahami alam semesta.
- 5. Data Lainnya
 - a. Data web mencakup konten situs web, riwayat pencarian, dan data clickstream, yang dapat digunakan untuk memahami perilaku online dan minat pengguna.
 - b. **Data medis seperti** rekam medis elektronik, gambar medis, dan data kesehatan lainnya, yang dapat digunakan untuk meningkatkan perawatan pasien dan penelitian medis.

6.2.2 Velocity

Kecepatan dalam menghasilkan data, memproses data dan menerima data merupakan ciri dari big data. Pada kasus big data, data dihasilkan secara *real-time* atau mendekati *real-time* berikut beberapa contoh dari data yang memiliki ciri khusus dalam hal *velocity* yaitu:

1. Data Cuaca dari Sensor seperti jaringan sensor yang ditempatkan di seluruh dunia, termasuk stasiun cuaca, balon udara, dan satelit. Contoh Jenis data: Temperatur, tekanan udara, kelembaban, kecepatan angin, arah angin, curah hujan, dan tutupan awan.
2. Data GPS dari Taksi seperti GPS yang terpasang pada armada taksi di kota besar. Contoh Jenis data: Lokasi taksi, waktu tempuh antar lokasi, dan pola pergerakan penumpang.
3. Komentar di Media Sosial seperti platform media sosial seperti Twitter, Facebook, dan Instagram. Contoh Jenis data:

Teks komentar, emoji, dan informasi pengguna yang berkomentar.

4. Riwayat Pencarian Pengguna. Mesin pencari seperti Google, Bing, dan DuckDuckGo. Contoh Jenis data: Istilah yang dicari pengguna, lokasi pengguna, dan waktu pencarian.
5. Data DNA seperti Proyek penelitian genomik manusia dan rumah sakit. Contoh Jenis data: Urutan kode genetik manusia.

Velocity merupakan tantangan dalam big data pada saat memproses dan menganalisis data sehingga dibutuhkan beberapa aplikasi dalam menangani hal tersebut berikut beberapa aplikasi yang dapat membantu kerangka kerja pemrosesan data *real-time* seperti *Apache Kafka*, *Apache Spark*, dan *Apache Flink*.

6.2.3 Variety

Variety merupakan aspek pada big data yang berbicara tentang keragaman jenis data yang akan dianalisis baik data terstruktur maupun data yang tidak terstruktur baik yang dihasilkan oleh manusia ataupun mesin. Tidak hanya itu data yang bersifat numerik, string, basis data tradisional hingga dokumen teks yang tidak terstruktur. Berikut beberapa sumber data yang beragam pada big data

1. Sumber tradisional seperti database, *spreadsheet*, dan aplikasi bisnis lainnya.
2. Sumber web seperti situs web, media sosial, dan platform online lainnya.
3. *Internet of Things* (IoT) seperti sensor yang terhubung ke internet yang menghasilkan data secara *real-time*.
4. Media sosial seperti posting, komentar, dan interaksi pengguna di platform media sosial.
5. Dokumen dan email seperti dokumen internal, email, dan komunikasi tertulis lainnya.

6.2.4 Veracity

Kualitas dari big data menjadi perhatian khusus dikarenakan *Volume* yang besar serta variasi data serta kecepatan data yang

besar membuat *veracity* menjadi ciri penting dari big data. *Veracity* berkaitan dengan kualitas kualitas, akurasi serta kebersihan data dari *noise*. Banyak Teknik telah dikembangkan dalam menangani masalah *veracity* pada big data seperti data *cleansing*, data eksplorasi dan data *scrubbing*. Berikut beberapa hal yang perlu diperhatikan tentang *Veracity* dalam big data

1. *Veracity* sangat dipengaruhi oleh sumber data. Data yang dikumpulkan dari sumber yang tidak kredibel atau tidak terstandarisasi lebih mungkin mengandung kesalahan atau *noise*.
2. Proses yang penting pada penanganan big data adalah pembersihan dan perbaikan data sangat penting untuk memastikan *Veracity*. Hal ini meliputi identifikasi dan koreksi data yang hilang, tidak konsisten, atau salah format serta standarisasi data yang belum terstandarisasi.
3. Konsistensi data juga merupakan aspek yang perlu diperhatikan dalam hal *Veracity* suatu data. Data yang dikumpulkan dari berbagai sumber perlu dikonsistenkan agar dapat dianalisis secara akurat.
4. Keamanan data juga penting untuk *Veracity*. Langkah-langkah perlu diambil untuk melindungi data dari akses yang tidak sah dan modifikasi.

6.2.5 Value

Nilai dari data menjadi hal yang sangat penting dari aspek big data. Konsep *Value* pada big data tidak hanya bercerita tentang volume dan *Variety* dan kompleksitas datanya lebih dari itu konsep *Value* pada big data bercerita tentang manfaat yang didapatkan dari data tersebut. Berikut beberapa contoh *Value* dari big data

1. Mengubah data mentah menjadi wawasan yang berarti. Big data itu sendiri pada dasarnya adalah bahan mentah. Nilai sebenarnya terletak pada mengubahnya menjadi wawasan yang dapat ditindaklanjuti yang dapat menginformasikan pengambilan keputusan, meningkatkan proses, dan menciptakan peluang baru.
2. Mengekstrak nilai melalui analisis. Untuk membuka nilai tersebut diperlukan teknik analisis data. Ini bisa melibatkan

metode tradisional seperti analisis statistik atau teknik yang lebih canggih seperti *machine learning* dan kecerdasan buatan.

3. *Value* untuk tujuan yang beragam. Nilai data dapat bervariasi tergantung pada tujuan spesifik organisasi. Misalnya, menganalisis data pelanggan dapat memberikan wawasan untuk meningkatkan kampanye pemasaran, sementara menganalisis data sensor dari mesin dapat membantu memprediksi dan mencegah kegagalan peralatan.

6.3 Teknologi Pendukung Big Data

Big data memiliki lima karakteristik utama yang dikenal sebagai 5V: *Volume*, *Variety*, *Velocity*, *Veracity*, dan *Value*. Karakteristik ini menghadirkan berbagai tantangan dalam hal penyimpanan, pengelolaan, pemrosesan, dan analisis data dalam jumlah besar. Oleh karena itu, diperlukan berbagai teknologi canggih untuk mengatasi permasalahan big data secara efektif.



Gambar 6.2. Tools Big Data

(Sumber : <https://tisnanews.com/beberapa-tools-big-data-gratis-open-source-2022/>)

6.3.1 Infrastruktur Penyimpanan

1. *Hadoop Distributed File System* (HDFS) merupakan sistem file terdistribusi yang beroperasi pada cluster besar, memungkinkan akses data dengan throughput tinggi. Sistem ini memiliki toleransi tinggi terhadap kesalahan dan dirancang untuk bekerja dengan perangkat keras komoditas. HDFS menyimpan setiap file sebagai rangkaian blok yang direplikasi pada beberapa mesin dalam cluster untuk meningkatkan ketahanan terhadap kesalahan. Adapun ciri-ciri dari HDFS adalah *Scalable Storage for Large Files*, Replikasi, *Streaming Data Access* dan *File Appends* (Santoso, 2020)
2. *Data Warehouse* atau sering disebut dengan Gudang data yang merupakan database khusus yang terkonsolidasi dari beberapa sumber-sumber data berbagai sistem informasi yang ada pada perusahaan atau organisasi. Tujuan adanya data warehouse untuk menggabungkan data dari berbagai sumber didalam organisasi menjadi satu “Gudang” terpusat dengan demikian pengguna dapat menjalankan query dengan mudah, dapat membuat laporan dan melakukan analisis dengan efisien (Purwati, 2018).
3. *Data Lake*: Repositori pusat yang menyimpan semua data mentah dan terstruktur dari berbagai sumber, terlepas dari apakah data tersebut akan dianalisis segera. Tujuan utamanya adalah mengumpulkan semua data yang dihasilkan organisasi untuk mendapatkan pandangan yang lebih berharga dan terperinci. Konsep *Data Lake* kini menantang gudang data tradisional yang handal untuk menyimpan data kompleks yang heterogen (Khine and Wang, 2018).

6.3.2 Pemrosesan Data

1. *Apache Spark* merupakan kerangka kerja komputasi cluster *open-source* yang biasa digunakan menganalisis data. Banyak keunggulan Spark dibandingkan dengan Hadoop (Santoso, 2020). Berikut beberapa keunggulan Sprak jika dibandingkan dengan Hadoop:

- a. Komputasi cluster dalam memori: Spark memproses data dalam memori, yang membuatnya jauh lebih cepat daripada Hadoop yang memproses data di disk.
- b. Berbagai alat tingkat tinggi: Spark menyediakan berbagai alat untuk analisis data, seperti:
- c. Streaming Spark: Untuk pekerjaan streaming real-time
- d. Spark SQL: Untuk analisis data terstruktur
- e. MLlib: Perpustakaan pembelajaran mesin
- f. GraphX: Pemrosesan graf
- g. Kueri *real-time*, *batch*, dan interaktif: Spark mendukung berbagai jenis kueri, memungkinkan pengguna untuk menganalisis data dengan berbagai cara.

API untuk Scala, Java, dan Python: Spark menyediakan API untuk berbagai bahasa pemrograman, membuatnya mudah diakses oleh berbagai pengembang.

2. Apache Flink adalah mesin pemrosesan data streaming dan *batch open-source* yang dibangun di atas Java dan Scala. Flink memungkinkan pengembang untuk membangun aplikasi yang memproses data secara *real-time*, seperti analisis data streaming, dan data terstruktur dalam batch. Flink terkenal dengan beberapa keunggulannya, yaitu:
 - a. Pemrosesan Data Streaming dan Batch Terpadu: Flink mampu memproses data streaming dan batch secara terpadu dalam satu platform, menghilangkan kebutuhan untuk menggunakan alat yang berbeda untuk kedua jenis pemrosesan.
 - b. Performa Tinggi: Flink dirancang untuk performa tinggi, mampu memproses data streaming dengan latensi rendah dan batch data dalam skala besar secara efisien.
 - c. Skalabilitas: Flink dapat dibuat skala secara horizontal untuk menangani beban kerja yang besar, membuatnya ideal untuk aplikasi big data.
 - d. Kemudahan Penggunaan: Flink menyediakan API yang intuitif dan mudah digunakan, memungkinkan pengembang untuk membangun aplikasi pemrosesan data yang kompleks dengan cepat.

6.3.3 Analisis Data

1. **Machine Learning**, atau Mesin Pembelajaran, adalah cabang kecerdasan buatan yang berfokus pada **pembelajaran dari data**. Hal ini berarti ML mengembangkan sistem yang mampu **belajar secara mandiri** tanpa perlu diprogram secara berulang oleh manusia. Agar ML dapat menghasilkan output yang optimal, sistem ini membutuhkan **data yang valid** sebagai bahan pembelajaran (proses training) sebelum digunakan untuk pengujian (testing) (Imam Cholissodin *et al.*, 2021)
 - a. *Machine learning* (ML) dapat dibagi ke dalam beberapa kategori berdasarkan pendekatan pembelajarannya diantaranya, *Supervised Learning*, *Unsupervised Learning*, *Semi-Unseprvised Learning*, dan *Reinforcement learning*.
 - b. Pembagian *Machine Learning* berdasarkan Teknik yang digunakan seperti, *Deep Learning* dan *Ensemble Learning*
2. *Data mining* atau penambangan data, adalah proses mencari informasi penting yang tersembunyi dan belum diketahui dalam kumpulan data yang besar. Informasi yang digali ini bersifat implisit, artinya tidak secara eksplisit tercantum dalam data, melainkan perlu dianalisis dan diinterpretasikan untuk menemukan maknanya (Muslim *et al.*, 2019). *Data mining* memiliki hubungan erat dengan berbagai bidang, diantaranya:
 - a. Statistik: Teknik statistik digunakan untuk menganalisis data dan menemukan pola dan tren.
 - b. *Machine Learning* (Pembelajaran Mesin): Algoritma machine learning digunakan untuk membangun model yang dapat memprediksi atau mengklasifikasikan data baru.
 - c. *Pattern Recognition* (Pengenalan Pola): Teknik *pattern recognition* digunakan untuk menemukan pola dalam data yang kompleks.

- d. *Computing Algorithms* (Algoritma Komputasi): Algoritma komputasi yang efisien digunakan untuk memproses data dalam jumlah besar.
 - e. *Database Technology* (Teknologi Database): Teknologi database digunakan untuk menyimpan dan mengelola data yang besar.
 - f. *High Performance Computing* (Komputasi Kinerja Tinggi): Komputasi kinerja tinggi digunakan untuk memproses data dengan cepat dan efisien.
3. *Bisnis Intelligence* adalah tentang memanfaatkan data untuk membuat keputusan yang lebih baik. Ini tidak hanya terbatas pada dunia bisnis, tetapi dapat diterapkan dalam berbagai aspek kehidupan. BI memungkinkan kita untuk mengubah data menjadi insights yang dapat ditindaklanjuti, membantu kita memahami situasi dengan lebih baik dan membuat keputusan yang lebih terinformasi (Prahendratno *et al.*, 2023). Ada beberapa Konsep Bisnis Intelijen diantaranya adalah:
- a. Ekstrak Data Mentah
Komponen awal dari solusi Business Intelligence meliputi data dari penjualan, laporan keuangan, informasi gaji, dan sumber daya lainnya. Data dari berbagai sistem dalam organisasi, seperti CRM, ERP, dan file datar, tersebar di berbagai tempat. Oleh karena itu, solusi Business Intelligence menyediakan konektor yang efektif untuk mengintegrasikan semua sumber data ini ke dalam platform tunggal untuk analisis yang lebih mendalam.
 - b. Konsolidasi Informasi
Gudang data berfungsi untuk menggabungkan berbagai database yang berbeda sehingga dapat terbentuk hubungan antar data. Data dari berbagai sumber, seperti sistem transaksional dan basis data relasional, mengalir ke dalam gudang data untuk disatukan dan diproses lebih lanjut.

- c. Mengakses dan Menganalisis Data
Setelah data terpusatkan di satu tempat, pemahaman yang mendalam diperlukan. Solusi Business Intelligence memanfaatkan akses terhadap informasi tersebut, menguraikannya untuk mengidentifikasi tren dan pola, lalu menyajikannya secara intuitif untuk dipahami.
- d. Buat Pedoman Instrumen dan Laporan
Pedoman Instrumen dan laporan membawa informasi yang kompleks dan sulit dipahami, kemudian mengubahnya menjadi pola, tren, dan wawasan yang mudah dipahami. Alat-alat ini membantu memudahkan kerja sama di dalam organisasi dengan memungkinkan berbagi temuan dan penemuan.

DAFTAR PUSTAKA

- Imam Cholissodin *et al.* (2021) *AI , MACHINE LEARNING & DEEP LEARNING (Teori & Implementasi)*. 1st edn. Available at: link: <http://bit.ly/3piOnnU>.
- Khine, P.P. and Wang, Z.S. (2018) 'Data lake: a new ideology in big data era', *ITM Web of Conferences*, 17, p. 03025. doi:10.1051/itmconf/20181703025.
- Muslim, M.A. *et al.* (2019) *Data Mining Algoritma C4.5*. Edited by E. Listiana and N. Cahyani.
- Prahendratno, A. *et al.* (2023) *Business Intelegent*. 1st edn. Edited by Y. Agusd. Jambi: PT. Sonpedia Publishing Indonesia.
- Purwati, N. (2018) *Data Warehouse*. 1st edn. Lampung1: Darmajaya (DJ) Press Alamat.
- Safar Dwi Kurniawan, M.K. *et al.* (2024) *BIG DATA (Mengenal Big Data & Implementasinya di Berbagai Bidang)*. 1st edn. Edited by S.& Y. Agusdi. Jambi: PT. Sonpedia Publishing Indonesia.
- Santoso, J.T. (2020) *ANALISIS Big Data*. 1st edn. Semarang: Yayasan Prima Agus Teknik.

BAB 7

PEMANFAATAN MACHINE LEARNING DALAM IOT

Oleh Hamdan Gani

7.1 Pendahuluan

7.1.1 Definisi dan Konsep Dasar *Machine Learning* (ML)

ML adalah cabang dari kecerdasan buatan (*Artificial Intelligence*) yang fokus pada pengembangan sistem yang dapat belajar dari data yang diberikan. Definisi dan konsep dasar ML mencakup beberapa elemen:

1. *Definisi ML*

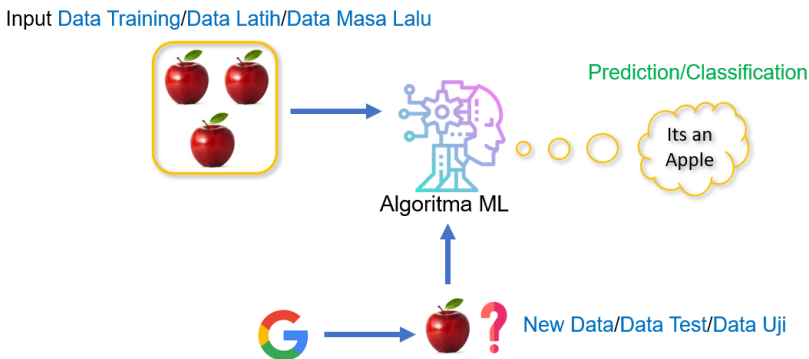
ML merujuk pada kemampuan sistem komputer untuk secara otomatis belajar dan meningkatkan kinerjanya tanpa menggunakan aturan yang secara eksplisit diprogram. Sistem ML mampu mengidentifikasi pola-pola kompleks dalam data dan membuat keputusan atau prediksi berdasarkan pembelajaran dari pengalaman (Firouzi et al., 2020).

2. *Konsep Dasar ML*

- a. *Data sebagai Input*: ML memanfaatkan data sebagai alat utamanya membuat sistem kecerdasan buatan. Data ini bisa berupa berbagai jenis, seperti gambar, teks, suara, atau data terstruktur dan tidak terstruktur lainnya.
- b. *Model dan Algoritma*: Model ML adalah representasi dari pengetahuan atau pemahaman yang diperoleh dari data yang telah dilatih. Algoritma ML adalah metode atau langkah-langkah yang diterapkan pada data untuk melatih model.
- c. *Pelatihan dan Pembelajaran*: Proses pelatihan (training) adalah tahap di mana model ML belajar dari data yang telah dikumpul. Model disesuaikan agar dapat menangkap pola dan hubungan dalam data.

- d. *Evaluasi dan Prediksi*: Setelah pelatihan, model dievaluasi menggunakan data baru yang tidak terlihat sebelumnya. Kemudian, model dapat digunakan untuk membuat prediksi atau keputusan terhadap data baru.
- e. *Supervised dan Unsupervised Learning*: *Supervised Learning*: Model dilatih menggunakan pasangan input-output, sehingga model dapat memprediksi output untuk data baru. *Unsupervised Learning*: Model mencoba mengidentifikasi pola tanpa menggunakan label atau informasi output. Algoritma klustering/pengelompokkan dan reduksi dimensi adalah contoh dari jenis ini.

Supervised Learning



Gambar 7.1. Supervised Learning
(Sumber: (Baduge et al., 2022))

Melalui konsep ini, ML memberikan kemampuan sistem untuk memahami pola dalam data, membuat keputusan atau prediksi, dan beradaptasi dengan perubahan atau data baru seiring waktu.

7.1.2 Definisi dan Konsep Dasar *Internet of Things* (IoT)

IoT merujuk pada jaringan perangkat fisik yang terhubung dan saling berkomunikasi melalui internet. Definisi dan konsep dasar IoT mencakup beberapa elemen utama:

1. *Definisi IoT*

IoT mengacu pada ekosistem di mana objek atau perangkat fisik dilengkapi dengan teknologi sensor, perangkat lunak, dan konektivitas internet untuk saling berkomunikasi dan bertukar data. Hal ini memungkinkan objek tersebut untuk mengumpulkan informasi, merespons lingkungan sekitar, dan bertindak secara otonom atau sesuai dengan instruksi (Hussain et al., 2020).

2. *Konsep Dasar IoT*

- a. *Objek Terhubung*: IoT melibatkan berbagai jenis objek atau perangkat yang dapat terhubung ke internet, mulai dari perangkat kecil seperti sensor hingga perangkat kompleks seperti kendaraan otonom dan perangkat rumah pintar.
- b. *Sensor dan Pengumpulan Data*: Perangkat IoT dilengkapi dengan sensor yang dapat mendeteksi berbagai parameter, seperti suhu, kelembaban, lokasi, gerakan, dan lainnya. Sensor ini memungkinkan perangkat untuk mengumpulkan data dari lingkungan sekitarnya.
- c. *Konektivitas Internet*: IoT memanfaatkan konektivitas internet untuk mentransfer data antar perangkat dan platform. Hal ini dapat melibatkan berbagai protokol komunikasi, termasuk Wi-Fi, Bluetooth, Zigbee, dan teknologi jaringan lainnya.
- d. *Interoperabilitas*: Konsep dasar IoT mencakup kemampuan perangkat untuk beroperasi dan berkomunikasi secara lintas platform dan vendor. Interoperabilitas memungkinkan integrasi yang lebih mudah antar perangkat dan sistem.
- e. *Cloud Computing*: Data yang dikumpulkan oleh perangkat IoT sering kali diproses dan disimpan di cloud. Cloud computing memungkinkan analisis data yang lebih canggih, penyimpanan yang berskala, dan akses data dari berbagai lokasi.
- f. *Analisis Data dan Keputusan Otomatis*: IoT memungkinkan analisis data secara real-time untuk mendapatkan wawasan yang lebih dalam. Dengan ML, keputusan

otomatis dapat diambil berdasarkan data yang diperoleh dari perangkat IoT.

- g. *Aplikasi Beragam*: Konsep dasar IoT mencakup berbagai aplikasi, seperti Smart Home (rumah pintar), Smart Cities (kota pintar), Industrial IoT (IoT industri), kesehatan digital, pertanian pintar, dan banyak lagi. Ini menciptakan ekosistem yang luas dan beragam.
- h. *Keamanan dan Privasi*: Mengingat jumlah besar data yang dihasilkan oleh perangkat IoT, keamanan dan privasi menjadi aspek penting. Konsep dasar IoT mencakup strategi keamanan yang ketat untuk melindungi data dan perangkat dari ancaman siber.

IoT telah membawa perubahan besar dalam cara kita berinteraksi dengan dunia di sekitar kita, membuka peluang baru untuk inovasi, efisiensi, dan kenyamanan. Konsep dasar ini terus berkembang seiring dengan evolusi teknologi dan penerapan IoT di berbagai sektor kehidupan. Dengan menggabungkan kecerdasan buatan melalui ML dengan konektivitas dan data dari IoT, organisasi dapat mencapai tingkat otomatisasi dan kecerdasan yang lebih tinggi, memberikan dampak positif pada berbagai sektor industri.

7.2 Integrasi ML dalam Ekosistem IoT

7.2.1 Keuntungan penggunaan ML dalam analisis data IoT

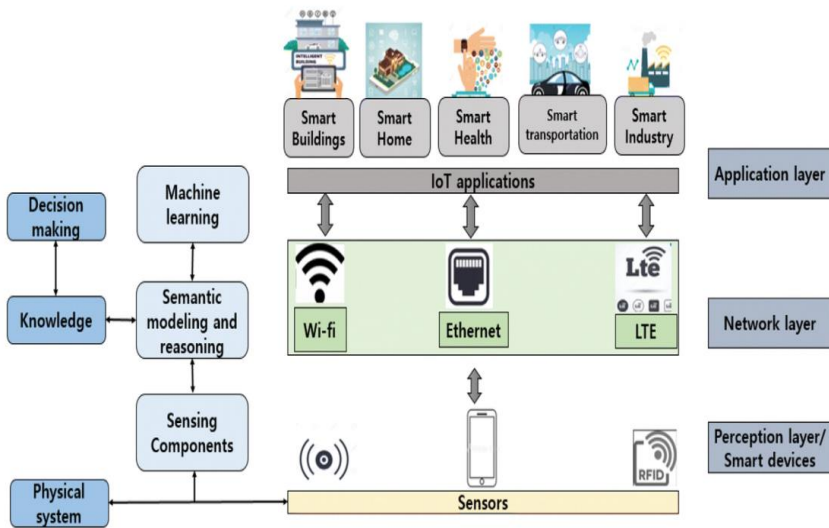
Penggunaan ML dalam analisis data IoT memberikan sejumlah keuntungan signifikan. Berikut adalah beberapa keuntungan utama dari menggabungkan ML dengan data yang dihasilkan oleh perangkat IoT (Sharma & Nandal, 2019):

- 1. *Identifikasi Pola yang Kompleks*: ML memungkinkan pengidentifikasian pola yang kompleks dalam data IoT, termasuk hubungan dan tren yang sulit dikenali secara manual. Hal ini membantu dalam memahami perilaku perangkat dan lingkungan IoT secara lebih mendalam.
- 2. *Prediksi dan Peramalan*: ML memungkinkan pembangunan model prediktif berdasarkan data historis yang dikumpulkan oleh perangkat IoT. Dengan menggunakan model ini, sistem

dapat membuat prediksi terkait performa perangkat, kejadian mendatang, atau kondisi lingkungan.

3. *Pemantauan Perawatan Prediktif*: ML dapat digunakan untuk menganalisis data kondisi dari perangkat IoT, pemantauan secara real-time. Juga memungkinkan prediksi waktu perawatan perangkat sehingga dapat mendeteksi potensi kegagalan alat sebelum terjadi, mengurangi downtime dan biaya perawatan.
4. *Optimasi Proses dan Efisiensi*: Dengan menganalisis data perangkat IoT, ML dapat membantu dalam mengoptimalkan proses operasional. Contohnya pengelolaan inventaris, dan penjadwalan produksi yang optimal.
5. *Personalisasi Layanan*: ML memungkinkan personalisasi layanan berdasarkan data pengguna. Dengan memahami preferensi/perilaku pengguna, sistem memberikan layanan rekomendasi produk dalam lingkungan IoT.
6. *Manajemen Energi yang Efisien*: Analisis ML dapat membantu dalam manajemen energi yang efisien. Sistem dapat mengidentifikasi pola konsumsi energi, memberikan saran untuk pengoptimalan dan pemborosan energi.
7. *Optimasi Jaringan dan Konektivitas*: ML dapat digunakan untuk mengoptimalkan kinerja jaringan IoT dengan memahami pola trafik, menyesuaikan kapasitas, dan meningkatkan efisiensi komunikasi antar perangkat.

Dengan menerapkan ML dalam analisis data IoT, organisasi/perusahaan dapat mengoptimalkan pengambilan keputusan, dan mendapatkan pengetahuan yang lebih mendalam dari lingkungan kerja teknologi IoT mereka. Sehingga, akan membantu di dalam memaksimalkan potensi penuh dari teknologi IoT dalam konteks pekerjaan mereka. Adapun arsitektur integrasi IoT dan ML dapat dilihat pada gambar 7.2.



Gambar 7.2. Integrasi IoT dan ML
(Sumber: (Phuyal et al., 2020))

7.2.2 Peningkatan efisiensi melalui ML dalam pengambilan keputusan

Peningkatan efisiensi melalui ML dalam pengambilan keputusan dapat dicapai dengan memanfaatkan kemampuan ML untuk menganalisis data, mengidentifikasi pola, dan membuat prediksi secara otomatis. Berikut adalah beberapa cara di mana ML dapat meningkatkan efisiensi dalam pengambilan keputusan (Rosati et al., 2023):

1. *Analisis Data yang Cepat dan Akurat:* ML dapat secara cepat menganalisis volume besar data yang dihasilkan oleh berbagai sumber, termasuk data historis dan data real-time dari perangkat IoT. Ini memungkinkan pengambilan keputusan berbasis fakta dan aktual.
2. *Prediksi dan Peramalan yang Akurat:* ML dapat membangun model prediktif untuk meramalkan hasil di masa depan berdasarkan pola-pola historis. Hal ini membantu dalam mengidentifikasi tren, mengantisipasi kejadian mendatang, dan membuat keputusan yang lebih tepat waktu.

3. *Optimasi Rantai Pasokan:* Dalam bisnis dan industri, ML dapat membantu mengoptimalkan rantai pasokan dengan memprediksi kebutuhan material, mengelola inventaris, dan meningkatkan efisiensi operasional keseluruhan.
4. *Manajemen Inventaris yang Efisien:* ML dapat membantu dalam pengelolaan inventaris dengan memberikan estimasi yang lebih akurat terkait stok yang diperlukan. Ini membantu mengurangi kelebihan persediaan dan meminimalkan kekurangan persediaan.
5. *Perawatan Pemeliharaan Prediktif:* Dalam lingkungan industri atau pemeliharaan peralatan, ML dapat digunakan untuk meramalkan waktu perawatan dan pemeliharaan yang optimal berdasarkan pemantauan kondisi perangkat. Ini mengurangi downtime yang tidak terduga dan meningkatkan ketersediaan perangkat.
6. *Personalisasi Layanan:* Dalam sektor layanan pelanggan atau pemasaran, ML dapat meningkatkan efisiensi dengan memberikan layanan yang lebih personal dan rekomendasi produk yang sesuai dengan preferensi individu pengguna.
7. *Pengoptimalan Proses Bisnis:* ML dapat digunakan untuk mengoptimalkan berbagai proses bisnis, termasuk otomatisasi tugas-tugas rutin dan pengidentifikasian peluang untuk meningkatkan produktivitas.
8. *Optimasi Energi dan Sumber Daya:* ML dapat membantu organisasi dalam mengoptimalkan penggunaan energi dan sumber daya dengan memahami pola konsumsi, memberikan saran untuk pengoptimalan, dan mengurangi pemborosan.
9. *Kesalahan dan Pemulihan Otomatis:* ML dapat mendeteksi kesalahan atau masalah operasional dengan cepat dan memberikan solusi otomatis atau memberikan rekomendasi untuk pemulihan.

Dengan memanfaatkan analisis data yang canggih dan kemampuan prediktif ML, organisasi dapat membuat keputusan yang lebih cepat, lebih tepat, dan lebih efisien. Peningkatan ini dapat menciptakan nilai tambah dan memberikan keunggulan kompetitif di berbagai industri dan konteks bisnis.

7.3 Contoh Kasus Penggunaan ML dalam IoT

7.3.1 Prediksi dan analisis data sensor

Contoh kasus penggunaan ML dalam IoT untuk prediksi dan analisis data sensor dapat ditemukan dalam berbagai industri. Berikut adalah contoh kasus tersebut:

1. *Pertanian Pintar (Smart Agriculture)*:
 - a. Tujuan: Meningkatkan produktivitas pertanian dan efisiensi penggunaan sumber daya.
 - b. Implementasi ML: Sensor tanah yang terhubung ke perangkat IoT mengukur tingkat kelembaban, pH tanah, dan suhu. Model ML dapat memprediksi kapan tanaman memerlukan irigasi berdasarkan data ini, dan memberikan rekomendasi untuk penggunaan air yang optimal (Shetty & Smitha, 2021).
2. *Manajemen Energi dalam Bangunan Pintar*:
 - a. Tujuan: Mengoptimalkan penggunaan energi dan meningkatkan efisiensi bangunan.
 - b. Implementasi ML: Sensor suhu, pencahayaan, dan kehadiran di bangunan terhubung ke sistem IoT. Model ML menganalisis data ini untuk memprediksi pola konsumsi energi, mengidentifikasi potensi pemborosan, dan memberikan saran untuk penjadwalan sistem pemanas dan pendingin secara optimal (Mazhar et al., 2022).
3. *Predictive Maintenance pada Mesin Industri*:
 - a. Tujuan: Mengurangi downtime dan biaya pemeliharaan mesin industri.
 - b. Implementasi ML: Sensor suhu, getaran, dan kecepatan di mesin industri mengumpulkan data terus-menerus. Model ML menggunakan data ini untuk memprediksi waktu pemeliharaan yang optimal, mendeteksi tanda-tanda potensi kegagalan, dan memberikan peringatan dini kepada operator (Çinar et al., 2020).
4. *Pemantauan Kesehatan Pasien Jarak Jauh*:
 - a. Tujuan: Memberikan pemantauan kesehatan pasien secara *real-time* dan meningkatkan perawatan pasien.
 - b. Implementasi ML: Sensor kesehatan terhubung ke perangkat IoT mengukur parameter kesehatan seperti

detak jantung, tekanan darah, dan suhu. Model ML memproses data ini untuk mendeteksi pola yang mencurigakan atau perubahan yang signifikan, memberikan informasi kepada dokter atau sistem kesehatan untuk tindakan lebih lanjut (Aldahiri et al., 2021).

5. *Jaringan Transportasi Cerdas:*

- a. Tujuan: Mengoptimalkan manajemen lalu lintas dan meminimalkan kemacetan.
- b. Implementasi ML: Sensor lalu lintas, kamera pengawas, dan perangkat deteksi kecepatan di jalan raya terhubung ke sistem IoT. Model ML menganalisis data ini untuk memprediksi pola lalu lintas, mengidentifikasi kejadian yang tidak terduga, dan memberikan rekomendasi untuk pengaturan lalu lintas yang optimal (Zantalis et al., 2019).

6. *Manajemen Kualitas Udara di Kota Pintar:*

- a. Tujuan: Memantau dan meningkatkan kualitas udara di lingkungan perkotaan.
- b. Implementasi ML: Sensor polusi udara, suhu, dan kelembaban terhubung ke sistem IoT di berbagai lokasi kota. Model ML mengolah data ini untuk memprediksi tingkat polusi udara, mengidentifikasi sumber polusi, dan memberikan informasi kepada warga dan pemerintah setempat (Zantalis et al., 2019).

Dengan memanfaatkan ML untuk menganalisis data sensor dari perangkat IoT, organisasi dapat meraih manfaat seperti pengambilan keputusan yang lebih tepat waktu, mengoptimalkan penggunaan sumber daya, dan pencegahan kegagalan perangkat. Hal ini membantu menciptakan solusi yang lebih cerdas dan adaptif dalam berbagai sektor.

7.3.2 Deteksi anomali dan keamanan IoT

Contoh kasus penggunaan ML dalam IoT untuk deteksi anomali dan keamanan melibatkan penerapan algoritma ML untuk mengenali perilaku yang tidak biasa atau potensi ancaman terhadap perangkat dan jaringan IoT. Berikut adalah skenario contoh:

1. *Deteksi Gerakan Yang Tidak Biasa Di Lingkungan Rumah*
 - a. Tujuan: Untuk mengidentifikasi pola gerakan yang tidak biasa (pencuri yang masuk ke lingkungan rumah)
 - b. Implementasi ML: Sensor gerak mengumpulkan data tentang aktivitas di sekitar rumah. Algoritma ML diprogram untuk mengidentifikasi pola gerakan yang tidak biasa, seperti gerakan yang terdeteksi di area yang jarang dilewati atau pada waktu yang tidak biasa (Hajla et al., 2023).
2. *Deteksi Akses Tidak Sah:*
 - a. Tujuan: memberikan peringatan jika terdeteksi akses yang tidak sah
 - b. Sensor pintu dan jendela digunakan untuk memantau akses ke rumah. ML digunakan untuk mempelajari pola akses normal penghuni rumah dan memberikan peringatan jika terdeteksi akses yang tidak sah, seperti pintu yang terbuka saat tidak seharusnya (Bokka & Sadasivam, 2021).
3. *Deteksi Perilaku Anomali:*
 - a. Tujuan: Memberikan peringatan dan mengambil tindakan preventif
 - b. Data dari semua sensor dikumpulkan dan dianalisis untuk mengidentifikasi perilaku anomali secara keseluruhan. Misalnya, jika terdeteksi sistem keamanan dimatikan saat pemilik rumah biasanya sedang berada di rumah, sistem akan memberikan peringatan dan mengambil tindakan preventif (Anthi et al., 2019).

Contoh diatas menjelaskan bagaimana ML digunakan bersama dengan IoT serta dalam konteks keamanan agar dapat membantu melindungi dan menjaga integritas jaringan serta perangkat terhubung dari potensi ancaman atau aktivitas yang tidak biasa. Deteksi dini dan respons cepat adalah kunci untuk menjaga keamanan dalam ekosistem IoT yang semakin kompleks.

7.4 Tantangan dan Hambatan dalam Pemanfaatan ML dalam IoT

7.4.1 Skala dan Volume Data

1. Penanganan big data dalam konteks IoT

Pemanfaatan ML dalam IoT membawa tantangan khusus terkait dengan skala dan volume data yang besar yang dihasilkan oleh perangkat IoT. Berikut adalah beberapa tantangan dan hambatan yang muncul dalam konteks penanganan Big Data dalam IoT (Bansal et al., 2021):

- a. *Volume Data yang Besar*: Perangkat IoT dapat menghasilkan jumlah data yang sangat besar, terutama ketika terdapat ribuan atau bahkan jutaan perangkat terhubung. Menangani volume data yang besar memerlukan infrastruktur dan kapasitas komputasi yang memadai.
- b. *Keterbatasan Infrastruktur*: Menyimpan, mengolah, dan menganalisis data dalam skala besar memerlukan infrastruktur komputasi dan penyimpanan yang mampu menangani beban kerja tinggi. Pergeseran ke model cloud computing seringkali diperlukan untuk mengatasi keterbatasan infrastruktur lokal.
- c. *Latensi dan Kecepatan*: Dalam beberapa kasus, seperti pengaturan yang membutuhkan respons real-time, penanganan data harus dilakukan dengan sangat cepat. Latensi yang rendah menjadi kunci untuk menjaga kinerja dan keakuratan sistem ML, dan ini dapat menjadi tantangan dalam skenario dengan keterbatasan jaringan.
- d. *Keseragaman dan Keragaman Data*: Data yang dihasilkan oleh perangkat IoT dapat sangat bervariasi dalam format, struktur, dan jenis. Menangani keragaman data ini memerlukan alat dan strategi yang efektif untuk pemrosesan data yang bersifat heterogen.
- e. *Keamanan dan Privasi*: Dengan meningkatnya volume data yang dikumpulkan, keamanan dan privasi menjadi perhatian utama. Memastikan bahwa data IoT tidak mudah diakses oleh pihak yang tidak berwenang, dan bahwa informasi sensitif terlindungi, adalah tantangan dalam pemanfaatan ML di lingkungan IoT.

- f. *Integrasi dan Interoperabilitas*: Perangkat IoT berasal dari berbagai vendor dengan protokol dan format data yang berbeda. Integrasi dan interoperabilitas yang efektif antara perangkat dan platform harus diatasi untuk memastikan penggunaan ML yang konsisten dan terkoordinasi.
- g. *Kualitas Data*: Data yang dihasilkan oleh perangkat IoT tidak selalu sempurna, dan bisa saja terdapat noise, ketidakpastian, atau ketidakakuratan. Meningkatkan kualitas data menjadi fokus utama untuk memastikan hasil analisis yang akurat.
- h. *Kesulitan dalam Menentukan Model ML yang Tepat*: Dalam lingkungan yang dinamis dan heterogen, menentukan model ML yang sesuai dapat menjadi kompleks. Pemilihan model yang tepat untuk menangani data dengan karakteristik tertentu merupakan tantangan sendiri.
- i. *Pemeliharaan dan Manajemen Model*: Pemeliharaan model ML yang digunakan untuk analisis data IoT memerlukan upaya terus-menerus. Model perlu diperbarui dan disesuaikan dengan perubahan dalam data atau kondisi lingkungan.

Pengelolaan tantangan ini memerlukan pendekatan holistik yang mencakup infrastruktur, kebijakan keamanan yang ketat, dan strategi manajemen data. Meningkatkan kapasitas organisasi untuk menangani skala dan volume data IoT menjadi kunci untuk kesuksesan pemanfaatan ML pada ekosistem IoT.

Tantangan pengolahan data real-time

Pemanfaatan ML dalam IoT, khususnya dalam konteks penanganan big data dan data real-time, dihadapkan pada sejumlah tantangan dan hambatan yang perlu diatasi. Berikut adalah beberapa tantangan utama yang terkait dengan pengolahan data dalam skala besar dan secara real-time dalam konteks IoT (Bian et al., 2022):

- a. *Volume Data yang Besar*:
 - 1) Tantangan: Perangkat IoT menghasilkan volume data yang sangat besar secara terus-menerus. Menangani volume

data yang besar memerlukan infrastruktur yang skalabel dan efisien.

- 2) Solusi: Penggunaan teknologi penyimpanan dan pemrosesan data yang canggih, seperti sistem distributed databases dan teknologi cloud, dapat membantu menangani volume data yang besar.

b. *Keterbatasan Bandwidth:*

- 1) Tantangan: Terkadang, keterbatasan bandwidth dapat menjadi hambatan dalam mentransfer data dari perangkat IoT ke pusat data untuk pengolahan lebih lanjut.
- 2) Solusi: Penerapan teknologi edge computing, di mana analisis data dilakukan di tepi jaringan (edge) sehingga hanya data yang relevan yang perlu dikirim ke pusat data, dapat membantu mengatasi keterbatasan bandwidth.

c. *Kecepatan Pemrosesan Real-Time:*

- 1) Tantangan: Pemrosesan data secara real-time memerlukan kecepatan dan responsivitas yang tinggi untuk menghasilkan hasil analisis dalam waktu yang sangat singkat.
- 2) Solusi: Pemilihan algoritma ML yang efisien secara komputasi dan pemilihan infrastruktur yang dapat memberikan kinerja real-time menjadi kunci dalam mengatasi tantangan ini.

d. *Keselarasan dan Sinkronisasi Data:*

- 1) Tantangan: Terdapat tantangan dalam menjaga keselarasan dan sinkronisasi data di antara perangkat IoT yang berbeda, terutama ketika data berasal dari berbagai sumber dan waktu.
- 2) Solusi: Implementasi protokol komunikasi yang solid, seperti MQTT atau CoAP, dan penggunaan teknologi seperti time-series databases dapat membantu menjaga integritas dan keselarasan data.

e. *Kesalahan dan Ketidakpastian Data:*

- 1) Tantangan: Data yang dihasilkan oleh perangkat IoT dapat mengandung noise, kesalahan, atau ketidakpastian, mempengaruhi kualitas analisis ML.
- 2) Solusi: Penggunaan teknik pra-pemrosesan data untuk membersihkan dan merapikan data, serta pengembangan model ML yang tahan terhadap ketidakpastian, dapat membantu mengatasi masalah ini.

f. *Integrasi Model ML yang Adaptif:*

- 1) Tantangan: Model ML harus dapat beradaptasi dengan perubahan dalam data dan lingkungan IoT, memerlukan integrasi yang dinamis dan pembaruan model secara berkala.
- 2) Solusi: Implementasi model ML yang dapat belajar secara online dan pembaruan model secara teratur untuk mencerminkan perubahan dalam data dan kondisi lingkungan.

g. *Biaya Infrastruktur dan Energi:*

- 1) Tantangan: Membangun dan memelihara infrastruktur yang memadai untuk menangani big data dan pemrosesan real-time dapat menjadi biaya yang signifikan. Selain itu, perangkat IoT yang membutuhkan daya dapat menjadi tantangan dari segi keberlanjutan dan efisiensi energi.
- 2) Solusi: Pilihan infrastruktur yang efisien dan scalable, bersama dengan inisiatif efisiensi energi untuk perangkat IoT, dapat membantu mengelola biaya dan dampak lingkungan.

h. *Ketergantungan pada Data Historis:*

- 1) Tantangan: Beberapa model ML bergantung pada data historis, dan tantangan muncul ketika data historis tidak mencerminkan kondisi atau situasi saat ini.
- 2) Solusi: Kombinasi data historis dengan data *real-time*, dan penggunaan teknik pembelajaran terhadap konsep (*concept drift*), dapat membantu meningkatkan responsivitas model terhadap perubahan kondisi.

Mengatasi tantangan ini memerlukan pendekatan holistik yang melibatkan pemilihan teknologi yang tepat, desain model ML yang cerdas, dan strategi implementasi yang efektif. Keberhasilan pemanfaatan ML dalam IoT tidak hanya bergantung pada kemampuan teknologi, tetapi juga pada manajemen data yang cermat, keamanan yang baik, dan kesadaran akan konteks bisnis dan lingkungan di mana solusi tersebut diterapkan.

7.4.3 Keamanan dan Privasi

1. Risiko keamanan yang terkait dengan implementasi ML dalam IoT

Implementasi ML dalam IoT membawa sejumlah risiko keamanan yang perlu diperhatikan secara serius. Dalam konteks IoT, di mana perangkat terhubung secara luas dan data yang dihasilkan mencakup informasi yang sangat berharga, risiko keamanan menjadi semakin signifikan. Berikut adalah beberapa risiko utama yang terkait dengan pemanfaatan ML dalam IoT (Abbas et al., 2022):

- a. *Serangan terhadap Model ML*: Model ML yang digunakan dalam IoT dapat menjadi target serangan. Serangan terhadap model dapat mencakup manipulasi data pelatihan atau data palsu dapat merusak kehandalan model.
- b. *Serangan terhadap Proses Pembelajaran (Adversarial Attacks)*: Adversarial attacks melibatkan pengiriman data yang dimodifikasi secara sengaja ke model ML dengan tujuan mengakibatkan keluaran yang tidak diinginkan atau salah.
- c. *Privasi Pengguna*: Pengolahan data pengguna oleh model ML dapat menimbulkan risiko privasi, terutama ketika data pribadi atau sensitif digunakan dalam pelatihan model.
- d. *Ketergantungan pada Data yang Tidak Aman*: Ketergantungan pada data yang tidak aman atau diperoleh dari sumber yang tidak tepercaya dapat membuka pintu bagi serangan atau manipulasi data yang merugikan.
- e. *Keamanan Perangkat IoT*: Perangkat IoT sendiri mungkin rentan terhadap serangan siber, seperti serangan terhadap perangkat keras atau perangkat lunak yang dapat

mempengaruhi operasional dan keamanan keseluruhan sistem.

- f. *Tanggung Jawab Model dan Interpretabilitas*: Model ML kompleks mungkin sulit untuk diinterpretasikan, dan sulit untuk menetapkan tanggung jawab jika keputusan model menciptakan dampak negatif.
- g. *Integrasi yang Tidak Aman*: Implementasi ML yang buruk atau integrasi yang tidak aman dalam arsitektur IoT dapat membuka celah keamanan, termasuk eksploitasi model ML melalui antarmuka atau protokol yang tidak aman.
- h. *Serangan terhadap Infrastruktur Komunikasi*: Serangan terhadap saluran komunikasi antar perangkat IoT dapat menyebabkan pencurian data, manipulasi data, atau serangan terhadap proses komunikasi.

Penting untuk diingat bahwa keamanan adalah tantangan yang dinamis dan harus dikelola secara terus-menerus seiring dengan perkembangan teknologi dan ancaman keamanan yang berkembang. Penerapan langkah-langkah pencegahan yang baik dapat membantu mengurangi risiko keamanan terkait implementasi ML dan IoT.

2. Strategi perlindungan data dan privasi

Perlindungan data dan privasi adalah aspek kritis dalam implementasi ML dalam IoT. Dengan perangkat IoT mengumpulkan dan memproses data yang sensitif, perlindungan data dan privasi menjadi prioritas utama. Berikut adalah beberapa strategi yang dapat diadopsi untuk melindungi data dan privasi dalam konteks implementasi ML pada IoT (Amiri-Zarandi et al., 2020):

- a. *Enkripsi Data*: Gunakan protokol enkripsi yang kuat seperti SSL/TLS untuk enkripsi data selama perjalanan. Selain itu, data yang disimpan di perangkat dan di pusat data harus dienkripsi.
- b. *Anonimisasi dan Pseudonimisasi*: Terapkan teknik anonimisasi atau pseudonimisasi pada data pribadi sebelum disimpan atau diproses. Pastikan bahwa data anonim atau

pseudonim tidak dapat dikaitkan kembali dengan individu tanpa informasi tambahan.

- c. *Kebijakan Akses yang Ketat*: Identifikasi dan berikan izin hanya kepada pengguna atau sistem yang membutuhkan data. Perbarui dan audit secara berkala kebijakan akses ini.
- d. *Pelatihan Kesadaran Keamanan*: Sediakan pelatihan reguler kepada tim pengembang, pengguna akhir, dan pemangku kepentingan terkait kebijakan dan praktik keamanan data.
- e. *Kontrol Pengguna*: Bangun antarmuka pengguna yang memungkinkan pengguna untuk mengontrol persetujuan dan preferensi privasi mereka.
- f. *Deteksi dan Respons Keamanan*: Terapkan perangkat lunak deteksi ancaman yang canggih dan prosedur respons keamanan yang cepat untuk menanggapi insiden segera.
- g. *Ketersediaan dan Pemulihan Data*: Lakukan cadangan rutin, pertahankan redundansi, dan implementasikan strategi pemulihan data yang dapat diandalkan.
- h. *Pemantauan dan Audit*: Implementasikan alat pemantauan dan sistem audit yang dapat melacak aktivitas data dan memberikan laporan secara teratur untuk evaluasi kepatuhan dan risiko.

Dengan menerapkan strategi ini, organisasi atau perusahaan dapat meminimalkan risiko terkait privasi dan melindungi data yang dikumpulkan dan diproses dalam implement.

7.5 Peluang dan Tren Masa Depan

Integrasi teknologi terbaru dalam ML dan IoT membawa inovasi yang signifikan dan membentuk fondasi untuk perkembangan teknologi masa depan. Berikut adalah beberapa inovasi dan pengembangan terkait (Abbas et al., 2022; Amiri-Zarandi et al., 2020):

1. *Edge AI (Artificial Intelligence)*: Edge AI membawa kemampuan kecerdasan buatan langsung ke perangkat IoT, memungkinkan analisis dan pengolahan data di tempat sumber data berada, tanpa memerlukan koneksi ke cloud.

2. *Federated Learning*: Federated Learning memungkinkan model ML untuk dilatih secara terdistribusi di berbagai perangkat IoT tanpa perlu mentransfer data ke pusat data sentral.
3. *Digital Twins*: Digital twins menciptakan representasi digital real-time dari objek fisik atau sistem, termasuk perangkat IoT, yang memungkinkan pemantauan, analisis, dan simulasi yang akurat.
4. *5G dan Komunikasi Nirkabel Tingkat Tinggi*: Implementasi teknologi 5G membawa konektivitas nirkabel tingkat tinggi, memungkinkan pertukaran data yang lebih cepat dan lebih handal antara perangkat IoT.
5. *AutoML (Automated ML)*: AutoML memanfaatkan kecerdasan buatan untuk otomatisasi tahap-tahap dalam proses pembuatan model ML, termasuk pra-pemrosesan, pemilihan fitur, dan penyesuaian parameter.
6. *Quantum Computing*: Quantum computing memanfaatkan sifat unik mekanika kuantum untuk memproses informasi dengan kecepatan yang jauh melampaui komputer klasik.
7. *Explainable AI (XAI)*: XAI menyediakan transparansi dan interpretabilitas dalam keputusan yang diambil oleh model ML, memungkinkan pengguna memahami alasan di balik prediksi atau keputusan model.
8. *Swarm Intelligence*: Inspirasi dari perilaku kelompok di alam seperti lebah dan semut, swarm intelligence menggabungkan prinsip ini untuk membuat jaringan perangkat IoT berkomunikasi dan berkoordinasi secara efisien.
9. *Blockchain dalam Keamanan*: Penerapan teknologi blockchain sebagai lapisan keamanan untuk melindungi data dan transaksi di perangkat IoT.
10. *Augmented Reality (AR) dan Virtual Reality (VR)*: Integrasi AR dan VR dengan perangkat IoT untuk memberikan pengalaman yang lebih interaktif dan imersif.

Integrasi teknologi terbaru dalam ML dan IoT membuka pintu bagi inovasi yang menciptakan solusi yang lebih cerdas, responsif, dan adaptif. Pengembangan ini tidak hanya mengoptimalkan kinerja dan efisiensi sistem, tetapi juga

memperluas ruang lingkup penggunaan teknologi ini dalam berbagai bidang, dari industri hingga kehidupan sehari-hari. Mendorong pengembangan teknologi ini dengan penuh tanggung jawab adalah kunci untuk memastikan bahwa dampaknya memberikan nilai tambah yang positif dan aman bagi masyarakat secara keseluruhan.

7.6 Kesimpulan

Pada bagian ini kita telah membahas secara rinci tentang pemanfaatan ML dalam IoT. Melalui berbagai studi kasus, kita dapat melihat bagaimana ML menjadi kunci dalam mengoptimalkan potensi IoT untuk berbagai aplikasi. Dari pembahasan dalam buku ini, beberapa kesimpulan utama dapat diambil. *Pendahuluan dan Definisi*: Memberikan pemahaman dasar bagi pembaca mengenai konsep ML dan IoT. Definisi yang jelas tentang konsep-konsep ini membantu dalam memahami peran dan pentingnya integrasi keduanya. *Integrasi ML dalam Ekosistem IoT*: Integrasi ML dalam ekosistem IoT memungkinkan analisis yang lebih cerdas dari data sensor dan informasi yang dikumpulkan. Ini memungkinkan sistem untuk belajar dari data secara mandiri dan membuat keputusan yang lebih baik secara otomatis. *Contoh Kasus Penggunaan*: Studi kasus yang disajikan memberikan gambaran yang nyata tentang bagaimana ML diterapkan dalam berbagai skenario IoT. *Tantangan dan Hambatan*: Tantangan yang dihadapi dalam pemanfaatan ML dalam IoT termasuk masalah privasi dan keamanan data, kompleksitas sistem, serta masalah interoperabilitas. *Peluang dan Tren Masa Depan*: Meskipun ada tantangan, namun banyak peluang yang terbuka dalam pemanfaatan ML dalam IoT. Kemajuan dalam teknologi dan inovasi akan terus memperluas cakupan aplikasi dan meningkatkan efisiensi sistem ML dan IoT.

Dengan demikian, materi ini memberikan wawasan tentang bagaimana pemanfaatan ML dalam IoT dan juga diharapkan materi ini dapat menjadi panduan bagi para praktisi, peneliti, dan pembaca buku lainnya yang tertarik dalam menggabungkan ML dengan teknologi IoT. Secara keseluruhan, integrasi sistem ML dan IoT memberikan peluang besar untuk meningkatkan daya saing dan efisiensi operasional organisasi/perusahaan. Dengan

perkembangan teknologi terus-menerus, integrasi ini dapat menjadi fondasi untuk mendukung pertumbuhan dan inovasi teknologi di masa depan.

DAFTAR PUSTAKA

- Abbas, G., Mehmood, A., Carsten, M., Epiphaniou, G., & Lloret, J. (2022). Safety, Security and Privacy in Machine Learning Based Internet of Things. *Journal of Sensor and Actuator Networks*, 11(3), 38. <https://doi.org/10.3390/jsan11030038>
- Aldahiri, A., Alrashed, B., & Hussain, W. (2021). Trends in Using IoT with Machine Learning in Health Prediction System. *Forecasting*, 3(1), 181–206. <https://doi.org/10.3390/forecast3010012>
- Amiri-Zarandi, M., Dara, R. A., & Fraser, E. (2020). A survey of machine learning-based solutions to protect privacy in the Internet of Things. *Computers & Security*, 96, 101921. <https://doi.org/10.1016/j.cose.2020.101921>
- Anthi, E., Williams, L., Slowinska, M., Theodorakopoulos, G., & Burnap, P. (2019). A Supervised Intrusion Detection System for Smart Home IoT Devices. *IEEE Internet of Things Journal*, 6(5), 9042–9053. <https://doi.org/10.1109/JIOT.2019.2926365>
- Baduge, S. K., Thilakarathna, S., Perera, J. S., Arashpour, M., Sharafi, P., Teodosio, B., Shringi, A., & Mendis, P. (2022). Artificial intelligence and smart vision for building and construction 4.0: Machine and deep learning methods and applications. *Automation in Construction*, 141, 104440. <https://doi.org/10.1016/j.autcon.2022.104440>
- Bansal, M., Chana, I., & Clarke, S. (2021). A Survey on IoT Big Data. *ACM Computing Surveys*, 53(6), 1–59. <https://doi.org/10.1145/3419634>
- Bian, J., Arafat, A. Al, Xiong, H., Li, J., Li, L., Chen, H., Wang, J., Dou, D., & Guo, Z. (2022). Machine Learning in Real-Time Internet of Things (IoT) Systems: A Survey. *IEEE Internet of Things Journal*, 9(11), 8364–8386. <https://doi.org/10.1109/JIOT.2022.3161050>
- Bokka, R., & Sadasivam, T. (2021). Deep Learning Model for Detection of Attacks in the Internet of Things Based Smart Home Environment. In *Advances in Intelligent Systems and Computing* (Vol. 1245, pp. 725–735). Springer.

- https://doi.org/10.1007/978-981-15-7234-0_69
- Çınar, Z. M., Abdussalam Nuhu, A., Zeeshan, Q., Korhan, O., Asmael, M., & Safaei, B. (2020). Machine Learning in Predictive Maintenance towards Sustainable Smart Manufacturing in Industry 4.0. *Sustainability*, 12(19), 8211. <https://doi.org/10.3390/su12198211>
- Firouzi, F., Farahani, B., Ye, F., & Barzegari, M. (2020). Machine Learning for IoT. In *Intelligent Internet of Things* (pp. 243–313). Springer International Publishing. https://doi.org/10.1007/978-3-030-30367-9_5
- Hajla, S. El, Mahfoud, E., Maleh, Y., & Mounir, S. (2023). Attack and anomaly detection in IoT Networks using machine learning approaches. *2023 10th International Conference on Wireless Networks and Mobile Communications (WINCOM)*, 7, 1–7. <https://doi.org/10.1109/WINCOM59760.2023.10322991>
- Hussain, F., Hussain, R., Hassan, S. A., & Hossain, E. (2020). Machine Learning in IoT Security: Current Solutions and Future Challenges. *IEEE Communications Surveys & Tutorials*, 22(3), 1686–1721. <https://doi.org/10.1109/COMST.2020.2986444>
- Mazhar, T., Malik, M. A., Haq, I., Rozeela, I., Ullah, I., Khan, M. A., Adhikari, D., Ben Othman, M. T., & Hamam, H. (2022). The Role of ML, AI and 5G Technology in Smart Energy and Smart Building Management. *Electronics*, 11(23), 3960. <https://doi.org/10.3390/electronics11233960>
- Phuyal, S., Bista, D., & Bista, R. (2020). Challenges, Opportunities and Future Directions of Smart Manufacturing: A State of Art Review. *Sustainable Futures*, 2(May), 100023. <https://doi.org/10.1016/j.sftr.2020.100023>
- Rosati, R., Romeo, L., Cecchini, G., Tonetto, F., Viti, P., Mancini, A., & Frontoni, E. (2023). From knowledge-based to big data analytic model: a novel IoT and machine learning based decision support system for predictive maintenance in Industry 4.0. *Journal of Intelligent Manufacturing*, 34(1), 107–121. <https://doi.org/10.1007/s10845-022-01960-x>
- Sharma, K., & Nandal, R. (2019). A Literature Study On Machine Learning Fusion With IOT. *2019 3rd International Conference*

- on *Trends in Electronics and Informatics (ICOEI)*, 2019-April, 1440–1445. <https://doi.org/10.1109/ICOEI.2019.8862656>
- Shetty, S., & Smitha, A. B. (2021). Smart Agriculture Using IoT and Machine Learning. In *Journal of Scientific Research and Technology* (pp. 1–16). https://doi.org/10.1007/978-981-16-6124-2_1
- Zantalis, F., Koulouras, G., Karabetsos, S., & Kandris, D. (2019). A review of machine learning and IoT in smart transportation. *Future Internet*, 11(4), 94. <https://doi.org/10.3390/FI11040094>

BAB 8

IMPLEMENTASI IOT PADA SMART HOME

Oleh Muhammad Fadli Azis

8.1 Konsep Smart Home

Smart Home merupakan kumpulan perangkat pintar yang saling bekerja sama dalam satu jaringan dan dapat dikendalikan dari jarak jauh. Semua perangkat pintar seperti lampu, termostat, kamera keamanan CCTV, dan peralatan-peralatan lainnya seperti yang terlihat pada Gambar 8.1, dikendalikan oleh sebuah pengendali otomatisasi rumah utama, yang sering disebut sebagai Smart Home hub. Hub ini adalah perangkat keras yang berfungsi sebagai titik pusat dari sistem rumah pintar dan dapat mendeteksi, memproses data, dan berkomunikasi secara nirkabel. Hub ini menggabungkan semua aplikasi yang terpisah menjadi satu aplikasi rumah pintar yang dapat dikendalikan oleh pemilik rumah secara jarak jauh. Contoh-contoh Smart Home hubs termasuk Amazon Echo dan Google Home (Yasar and Shea, 2023).

Perangkat rumah pintar dapat diprogram untuk mengikuti jadwal atau perintah tertentu. Perangkat ini dapat diatur untuk merespons perintah suara melalui asisten rumah seperti Amazon Alexa atau Google Assistant. Sebagai contoh, sebuah termostat pintar dapat mempelajari kebiasaan pemilik rumah dan secara otomatis menyesuaikan suhu berdasarkan jadwal secara spesifik. Dengan demikian, teknologi Smart Home tidak hanya memungkinkan kontrol yang lebih mudah dan efisien, tetapi juga memberikan kemampuan adaptasi yang cerdas sesuai dengan kebutuhan penghuni rumah.



Gambar 8.1. Perangkat pintar pada Smart Home
(Yasar and Shea, 2023)

8.2 Implementasi IoT pada Smart Home

Konsep utama dalam *Internet of Things* (IoT) adalah memungkinkan semua perangkat terhubung untuk berkomunikasi dan bertukar informasi melalui jaringan internet. Konsep ini juga dapat diterapkan pada Smart Home atau rumah pintar yang memungkinkan perangkat-perangkat pada rumah terhubung di internet, sehingga kita dapat melakukan pemantauan dan pengontrolan dari jarak jauh seperti pencahayaan pada lampu, keamanan pada kamera CCTV, penguncian pintu, dan sebagainya (Padmanaban et al., 2023).

Sebagai bagian dari *Internet of Things* (IoT), sistem dan perangkat Smart Home bekerja bersama, berbagi data penggunaan konsumen, dan mengotomatisasi berbagai tindakan berdasarkan preferensi pemilik rumah. Dengan integrasi IoT, perangkat pintar dalam rumah dapat beroperasi secara terintegrasi, saling berbagi data, dan berfungsi secara otomatis sesuai dengan keinginan penghuni. Hal ini tidak hanya menciptakan lingkungan rumah yang

lebih aman dan nyaman, tetapi juga membawa manfaat efisiensi energi yang signifikan. Dengan demikian, konsep Smart Home memberikan kemudahan dan keuntungan bagi pemilik rumah dalam kehidupan sehari-hari (Wang and Song, 2017).

8.3 Contoh Implementasi IoT pada Smart Home

Terdapat banyak perangkat elektronik pada rumah pintar yang terintegrasi dengan teknologi IoT. Semua perangkat tersebut diciptakan untuk memudahkan berbagai aktivitas di dalam rumah. Berikut adalah contoh beberapa perangkat IoT yang umum digunakan pada Smart Home (Telkomsel, 2022).

8.3.1 Smart Light

Smart Light adalah salah satu contoh implementasi IoT pada Smart Home yang dengan fitur pencahayaan yang cerdas dan terkoneksi seperti yang terlihat pada Gambar 8.2. Smart Light adalah lampu yang dapat terhubung ke jaringan internet, memungkinkan pengguna untuk mengontrolnya dari jarak jauh melalui aplikasi di perangkat pintar. Fitur-fitur yang dimiliki Smart Light berbasis IoT meliputi pengontrolan secara otomatis berdasarkan waktu atau peristiwa tertentu, pengaturan kecerahan sesuai dengan kondisi cahaya sekitar atau mendeteksi kehadiran orang di ruangan untuk mengaktifkan atau mematikan lampu secara otomatis.



Gambar 8.2. Smart Light
(Bardi, 2024)

8.3.2 Smart Plug

Smart Plug merupakan contoh lain dari implementasi IoT pada Smart Home yang menghadirkan kecerdasan pada soket listrik seperti yang terlihat pada Gambar 8.3. Dengan menggunakan teknologi IoT, *Smart Plug* memungkinkan pengguna untuk mengontrol perangkat listrik yang terhubung ke soket tersebut secara remote melalui aplikasi di perangkat pintar mereka. Fitur-fitur yang dimiliki oleh *Smart Plug* antara lain fitur untuk mematikan atau menghidupkan perangkat secara otomatis berdasarkan waktu atau kondisi tertentu dan memantau konsumsi energi dari perangkat yang terhubung.



Gambar 8.3. Smart Plug
(Bardi, 2024)

9.3.3 Smart Door Lock

Smart Door Lock adalah contoh lain dari penerapan teknologi IoT dalam Smart Home yang menghadirkan keamanan dan kenyamanan tambahan bagi penghuninya seperti yang terlihat pada Gambar 8.4. Smart Door Lock memungkinkan pengguna untuk mengontrol akses pintu masuk rumah mereka secara remote melalui aplikasi di perangkat pintar mereka. Fitur-fitur yang dimiliki oleh Smart Door Lock mencakup kemampuan untuk membuka atau mengunci pintu dari jarak jauh, memberikan akses sementara kepada tamu atau anggota keluarga dengan kode akses unik atau melalui aplikasi, serta memberikan notifikasi kepada pengguna ketika pintu terbuka atau terkunci.



Gambar 8.4. Smart Door Lock
(Bardi, 2024)

8.3.4 Smart Security Camera

Smart Security Camera adalah salah satu contoh penerapan teknologi IoT dalam Smart Home yang memberikan pengguna kemampuan untuk memantau rumah mereka secara real-time dari jarak jauh melalui aplikasi di perangkat pintar mereka seperti yang terlihat pada Gambar 8.5. Fitur-fitur yang dimiliki oleh Smart Security Camera meliputi kemampuan merekam video berkualitas tinggi, mendeteksi gerakan atau aktivitas yang mencurigakan, memberikan notifikasi kepada pengguna ketika ada aktivitas yang terdeteksi, dan memungkinkan pengguna untuk berkomunikasi dua arah melalui speaker dan mikrofon yang terpasang pada kamera.



Gambar 8.5. Smart security camera
(Bardi, 2024)

8.3.5 Smart Appliances

Smart Appliances adalah contoh lain dari implementasi IoT pada Smart Home yang membawa inovasi ke dalam perangkat rumah tangga tradisional. Perangkat rumah tangga seperti mesin cuci, kulkas, oven, dan peralatan lainnya dapat ditingkatkan ke tingkat berikutnya dengan teknologi IoT seperti yang terlihat pada Gambar 8.6. Fitur-fitur yang dimiliki oleh Smart Appliances meliputi kemampuan untuk terhubung ke jaringan internet, memungkinkan pengguna untuk mengontrol dan memantau perangkat dari jarak jauh melalui aplikasi di perangkat pintar mereka. Selain itu, Smart Appliances juga dapat dilengkapi dengan sensor-sensor cerdas yang memungkinkan mereka untuk mengatur penggunaan energi secara otomatis, memberikan notifikasi ketika perawatan atau perbaikan diperlukan, dan bahkan belajar pola penggunaan pengguna untuk meningkatkan efisiensi dan kenyamanan.



Gambar 8.6. Smart Appliances
(Samsung, 2024)

8.3.6 Smart Pet Feeder

Smart Pet Feeder adalah salah satu contoh penerapan teknologi IoT dalam Smart Home yang memberikan kemudahan bagi pemilik hewan peliharaan untuk memberi makan hewan

peliharaan mereka secara terjadwal dan terkontrol seperti yang terlihat pada Gambar 8.7. Smart Pet Feeder dilengkapi dengan fitur-fitur cerdas yang memungkinkan pengguna untuk mengatur jadwal pemberian makan, memberikan porsi makan yang tepat, dan bahkan memberikan notifikasi kepada pengguna ketika makanan hewan peliharaan sudah habis atau perlu diisi ulang. Dengan koneksi internet, pengguna dapat mengontrol Smart Pet Feeder dari jarak jauh melalui aplikasi di perangkat pintar mereka, memastikan bahwa hewan peliharaan mereka mendapatkan makanan yang cukup meskipun pengguna sedang tidak berada di rumah. Integrasi IoT pada Smart Pet Feeder juga memungkinkan pengguna untuk memantau pola makan hewan peliharaan mereka dan memberikan perawatan yang lebih baik secara keseluruhan.



Gambar 8.7. Smart Pet Feeder
(Bardi, 2024)

8.3.7 Smart Speaker

Smart Speaker adalah perangkat pintar yang memiliki kemampuan untuk berfungsi sebagai asisten virtual dan pengendali perangkat lain dalam Smart Home seperti yang terlihat pada Gambar 8.8. Dengan teknologi IoT, Smart Speaker dapat terhubung ke jaringan rumah pintar dan mengintegrasikan berbagai fungsi yang berguna bagi pengguna. Fitur-fitur yang dimiliki oleh Smart Speaker meliputi kemampuan untuk menjawab pertanyaan, memutar musik atau audiobook, memberikan informasi cuaca, dan mengeksekusi perintah suara untuk mengontrol perangkat lain

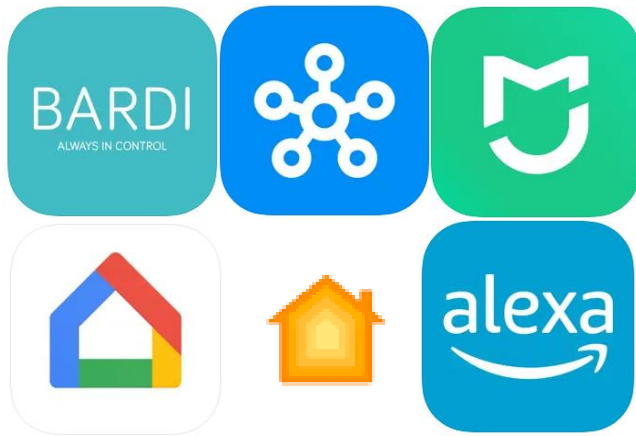
dalam rumah. Dengan menggunakan aplikasi atau platform yang sesuai, pengguna dapat memanfaatkan Smart Speaker untuk membuat rutinitas otomatis, mengatur alarm, atau bahkan mengatur penerangan dan suhu dalam ruangan dengan perangkat lain yang terhubung. Dengan integrasi IoT, Smart Speaker dapat menjadi pusat kontrol pintar yang efisien dan memberikan pengalaman pengguna yang lebih menyeluruh dalam mengelola rumah pintar mereka.



Gambar 8.8. Smart Speaker
(Google Store, 2024)

8.4 Platform IoT Smart Home

Platform IoT Smart Home adalah sistem yang memungkinkan pengguna untuk menghubungkan, mengontrol, dan memantau perangkat rumah pintar mereka melalui jaringan internet. Platform-platform ini memberikan kemudahan bagi pengguna untuk mengontrol dan mengelola perangkat rumah pintar mereka dengan lebih efisien melalui aplikasi (*software*) yang dapat diinstal pada smartphone seperti yang terlihat pada Gambar 8.9. Selain itu, platform IoT Smart Home juga mencakup perangkat keras (*hardware*) yang mendukung fungsionalitas ini, serta dapat diintegrasikan dengan perangkat keras dari berbagai brand. Berikut adalah beberapa platform IoT Smart Home yang paling umum digunakan saat ini.



Gambar 8.9. Platform IoT Smart Home
(Apple, 2024)

8.4.1 Bardi Smart Home

Bardi Smart Home adalah platform lokal dari Indonesia. Bardi menyediakan solusi rumah pintar yang dapat diandalkan dan mudah digunakan. Melalui aplikasi Bardi Smart Home, pengguna dapat mengontrol perangkat rumah pintar mereka dengan cepat dan efisien.

8.4.2 Samsung SmartThings

Samsung *SmartThings* adalah platform yang menyediakan integrasi dengan berbagai perangkat rumah pintar dari berbagai merek. Melalui aplikasi *SmartThings*, pengguna dapat menghubungkan dan mengontrol perangkat mereka, serta membuat rutinitas dan mengatur aksi otomatis.

8.4.3 Xiaomi Smart Home

Xiaomi Smart Home adalah platform dengan berbagai perangkat rumah pintar yang terjangkau dan fungsional. Pengguna dapat mengontrol perangkat Xiaomi mereka melalui aplikasi Mi Home, yang menyediakan pengaturan dan kontrol yang mudah serta integrasi dengan berbagai perangkat Xiaomi lainnya.

8.4.4 Google Home

Google Home adalah asisten suara yang dikembangkan oleh Google dan dapat diakses melalui perangkat seperti Google Home atau smartphone. Melalui aplikasi Google Home, pengguna dapat menghubungkan, mengatur, dan mengontrol perangkat rumah pintar, serta membuat rutinitas berdasarkan preferensi pengguna.

8.4.5 Apple HomeKit

Apple HomeKit adalah platform yang dikembangkan oleh Apple untuk menghubungkan dan mengontrol perangkat rumah pintar yang kompatibel dengan produk-produk Apple seperti iPhone, iPad, dan Apple Watch. Aplikasi Home memungkinkan pengguna untuk mengatur perangkat rumah pintar, membuat skenario otomatis, dan memantau rumah mereka secara jarak jauh.

8.4.6 Amazon Alexa

Amazon Alexa adalah platform asisten suara yang terintegrasi dengan berbagai perangkat rumah pintar. Pengguna dapat mengontrol perangkat mereka dengan perintah suara melalui perangkat Alexa, seperti Amazon Echo. Aplikasi yang terkait, Amazon Alexa, memungkinkan pengguna untuk mengatur perangkat, membuat rutinitas, dan mengakses berbagai fitur-fitur lainnya.

DAFTAR PUSTAKA

- Apple, 2024. App Store. URL <https://www.apple.com/app-store/>
- Bardi, 2024. Products. URL <https://bardi.co.id/products/>
- Google Store, 2024. Google Nest speakers and displays. URL https://store.google.com/gb/product/google_nest_mini?hl=en-GB
- Padmanaban, S., Nasab, Mostafa Azimi, Shiri, M.E., Javadi, H.H.S., Nasab, Morteza Azimi, Zand, M., Samavat, T., 2023. The Role of Internet of Things in Smart Homes, in: Artificial Intelligence-Based Smart Power Systems. pp. 259–271. <https://doi.org/10.1002/9781119893998.ch13>
- Samsung, 2024. Home Appliances. URL <https://www.samsung.com/id/home-appliances/>
- Telkomsel, 2022. 7 Contoh IoT dalam Konsep Teknologi Smart Home. URL <https://www.telkomsel.com/jelajah/jelajah-lifestyle/7-contoh-iot-dalam-konsep-teknologi-smart-home>
- Wang, G., Song, D., 2017. SMART HOME SERVICES USING THE INTERNET OF THINGS, in: Internet of Things and Data Analytics Handbook. pp. 613–630. <https://doi.org/10.1002/9781119173601.ch37>
- Yasar, K., Shea, S., 2023. Smart Home. URL <https://www.techtarget.com/iotagenda/definition/smart-home-or-building>

BAB 9

IMPLEMENTASI IOT PADA SMART CITY

Oleh Asma Ainuddin

9.1 Smart City

Smart City, atau yang dikenal sebagai Kota Pintar, adalah sebuah kota yang mengintegrasikan teknologi canggih untuk meningkatkan kesejahteraan masyarakatnya. Dengan berbagai sistem yang telah dikembangkan, kota pintar dapat mengurangi beban biaya pemerintah dan meningkatkan efisiensi dalam berbagai aspek kehidupan kota. Penerapan konsep kota pintar meliputi beragam bidang dan telah menjadi bagian dari kehidupan sehari-hari bagi warga kota. Salah satu keuntungan utama dari adopsi konsep kota pintar adalah daya tariknya bagi pengunjung, baik dari dalam maupun luar negeri, yang tertarik melihat kemajuan dan teknologi canggih yang dimiliki oleh kota tersebut.

Meskipun demikian, ada beberapa tantangan yang harus dihadapi dalam mengimplementasikan konsep kota pintar. Salah satunya adalah perlunya penegakan hukum yang ketat karena setiap pelanggaran terekam oleh sistem dan sulit untuk disembunyikan. Meskipun demikian, banyak kota maju di seluruh dunia telah mengadopsi konsep kota pintar. Contohnya adalah Republik Rakyat Tiongkok, di mana berbagai sistem seperti lampu lalu lintas pintar dan zebra cross pintar telah diterapkan di berbagai kota. Konsep kota pintar menjadi pilihan strategis bagi kota-kota yang ingin meningkatkan kualitas hidup dan memanfaatkan teknologi untuk kepentingan masyarakat (Arman, 2019).

Ide pembangunan kota pintar bermula pada tahun 1960an dan 1970an, saat *Community Analysis Bureau* mulai menggunakan teknologi seperti basis data komputer, analisis klaster, dan foto udara inframerah untuk mengumpulkan data. Mereka menggunakan data ini untuk menerbitkan laporan dan

mengalokasikan sumber daya ke daerah yang membutuhkan, dengan tujuan mengurangi risiko bencana dan mengatasi kemiskinan. Dari sana, muncul tiga generasi berbeda dari konsep kota pintar (Shea, 2020).

1. Pada generasi awal, Smart City 1.0, perusahaan teknologi menjadi pionir. Mereka fokus pada penggunaan teknologi di kota, walaupun pemerintah kota mungkin tidak sepenuhnya memahami implikasi atau dampaknya.
2. Generasi ke-dua, Smart City 2.0, pemerintah kota ikut ambil bagian dalam menggagas masa depan kota dengan teknologi pintar dan inovasi lainnya.
3. Generasi ke-tiga, Smart City 3.0, melibatkan kolaborasi antara penyedia teknologi, pemerintah kota, dan warga. Model ini menekankan partisipasi aktif warga dalam menciptakan komunitas cerdas yang inklusif. Contoh implementasi model ke-tiga ini dapat dilihat di Wina, Austria, di mana kemitraan antara pemerintah kota dan perusahaan energi lokal melibatkan warga sebagai investor di pembangkit listrik tenaga surya. Di samping itu, Vancouver, Kanada, melibatkan ribuan warga dalam penyusunan rencana aksi untuk menjadi kota paling hijau pada tahun 2020.

9.2 Konsep SMART City

Smart City dapat dilihat dalam berbagai aspek diantaranya pemerintahan cerdas (*smart government*), ekonomi cerdas (*smart economy*), kehidupan sosial cerdas (*smart society*), mobilitas cerdas (*smart mobility*), lingkungan cerdas (*smart environment*), dan kualitas hidup (*quality of live*) yang tinggi. Model ini sejalan dengan kerangka kerja *Smart City* yang diterapkan di Indonesia, yang juga mengusung enam pilar (Setiawan and Aindita, 2022) atau disebut juga sebagai enam karakteristik antara lain (Angelakis *et al.*, 2017):

1. *Smart Governance*

Mengadopsi konsep Sistem Pemerintahan Berbasis Elektronik dimulai dengan tujuan memperkenalkan dan membiasakan masyarakat dengan pelayanan digital.

2. *Smart Society*

Memahami dengan cermat potensi dan keunggulan wilayah sambil tetap menjunjung norma dan etika yang telah dianut oleh masyarakatnya.

3. *Smart Living*

Menyediakan lingkungan yang ramah dan aman bagi seluruh masyarakat dengan menyediakan fasilitas dan infrastruktur yang berkualitas dan terawat dengan baik.

4. *Smart Economy*

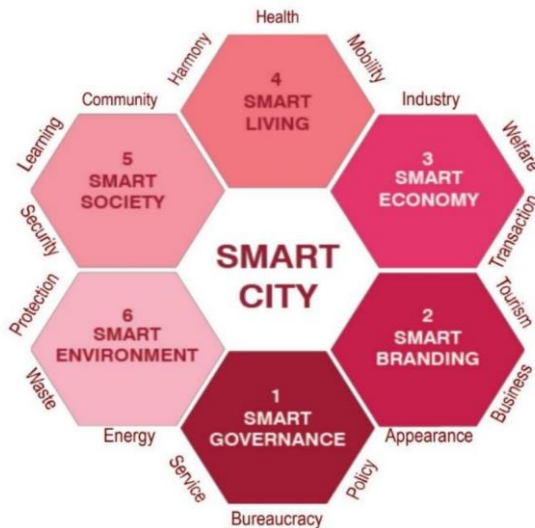
Menjamin bahwa sektor ekonomi memanfaatkan sepenuhnya teknologi yang ada untuk mencapai tingkat stabilitas ekonomi yang diinginkan di tingkat daerah.

5. *Smart Environment*

Membuat suasana yang nyaman sambil tetap menjaga keteraturan dan kebersihan.

6. *Smart Branding*

Memahami dan menetapkan identitas suatu wilayah untuk membangun citra yang mudah dikenali, yang juga bisa menjadi sumber motivasi untuk mencapai tujuan yang diinginkan.



Gambar 9.1. Konsep Smart City

(Sumber: Smart Nation, Mastering Nation's Advancement from Smart Readiness to Smart City)

9.3 Penerapan Smart City Pada Kota Besar Di Indonesia

Kota-kota besar di Indonesia memang memiliki banyak kesamaan, tetapi implementasi konsep Smart City di setiap kota tersebut ternyata didasarkan pada latar belakang yang berbeda. Misalnya, penerapan Smart City di Jakarta dan Surabaya memiliki perbedaan, begitu pula dengan Bandung dan Yogyakarta. Fokus Smart City juga berbeda-beda di setiap kota, dipengaruhi oleh potensi daerah seperti sumber daya alam dan sumber daya manusia. Hal ini memengaruhi dari mana proses pembangunan Smart City dimulai. Oleh karena itu, penting untuk melakukan penelitian dan analisis mendalam terkait konsep Smart City dan potensi daerah setempat sebelum implementasinya dilakukan (Puspitasari, 2021). Beberapa kota besar dengan konsep smart city-nya dijelaskan sebagai berikut:

9.3.1 Jakarta

Dalam upaya untuk mengubah Jakarta menjadi kota cerdas versi 4.0, Pada tahun Pemerintah Provinsi DKI Jakarta mendirikan Jakarta Smart City. Jakarta Smart City merupakan Badan Layanan Umum Daerah (BLUD) yang berada di bawah Dinas Komunikasi, Informatika, dan Statistik (Diskominfotik) Provinsi DKI Jakarta. Tugas utamanya adalah untuk memanfaatkan teknologi secara optimal dalam urusan pemerintahan dan pelayanan publik. Semua kebijakan terkait Jakarta Smart City diatur dalam Peraturan Gubernur Nomor 280 Tahun 2014 tentang Pembentukan, Organisasi, dan Tata Kerja Unit Pengelola Jakarta Smart City.

Jakarta Smart City beroperasi berdasarkan enam indikator yang telah ditetapkan sebelumnya, yakni *smart governance*, *smart economy*, *smart environment*, *smart people*, *smart mobility*, dan *smart living*. Indikator-indikator ini menjadi landasan bagi produk dan layanan yang disediakan oleh Jakarta Smart City. Produk layanan yang dimaksud antara lain (Sofa, 2023):

1. Indikator smart Governance diwujudkan dengan produk layanan antara lain: JAKI, Cepat Respons Masyarakat, Pantau Banjir, Peta Jakarta Kini, Digital Xperience, Data Science Trainee, Sistem Pemerintahan Berbasis Elektronik (SPBE),

Sistem Pemerintahan Berbasis Elektronik (SPBE), Kebijakan berbasis data.

2. Indikator smart economy diwujudkan dengan produk layanan antara lain: JakPreneur, Transaksi Digital UMKM.
3. Indikator smart environment diwujudkan dengan produk layanan antara lain: Pengendalian banjir dengan Flood Control System, Transportasi umum berbasis listrik,
4. Indikator smart mobility diwujudkan dengan produk layanan antara lain: Pembangunan Transit Oriented Development(TOD), Integrasi Sistem Pembayaran Transportasi Umum.
5. Indikator smart living diwujudkan dengan produk layanan antara lain: JakSehat, JakSehat.
6. Indikator smart branding diwujudkan dengan produk layanan antara lain: Enjoy Jakarta, Jakarta sebagai Kota Global.

9.3.2 Surabaya

Pemkot Surabaya mengadopsi konsep Smart City dengan dasar pada Instruksi Presiden Nomor 3 Tahun 2003 tentang Kebijakan dan Strategi Nasional Pengembangan E-Government. Dalam upaya menerapkan konsep Smart City, Pemerintah Kota Surabaya telah merancang beberapa program kegiatan untuk mencapai tujuan yang terkandung dalam konsep tersebut. Program kegiatan yang dimaksud antara lain (Amalia, Nesya and Tyrta, 2023):

1. *Smart government*, pemerintah dapat menciptakan layanan yang lebih transparan dan akuntabel bagi masyarakat. Hal ini dapat mempermudah proses pemberian layanan publik di Kota Surabaya.
2. *Smart branding* dapat meningkatkan daya saing daerah dengan penataan kota yang rapi dan pemasaran potensi daerah secara lokal, nasional, dan internasional. Salah satu contohnya adalah program Sparkling Surabaya.
3. *Smart economy* yang diwujudkan oleh Pemerintah Kota Surabaya dengan menjadikan kota sebagai pusat perekonomian kreatif dan berdaya saing.

4. *Smart living* melalui kegiatan yang memperhatikan harmonisasi tata ruang dan kesehatan masyarakat. Salah satunya adalah pengembangan program kampus merdeka di Kota Surabaya.
5. *Smart society* diwujudkan melalui penertiban angkutan umum untuk meningkatkan kualitas layanan transportasi bagi masyarakat.
6. *Smart environment*, Kota Surabaya dapat memperhatikan pelestarian lingkungan dan penerapan kebijakan yang ramah lingkungan.

9.3.3 Yogyakarta

Implementasi program Jogja Smart City di Kota Yogyakarta telah memberikan dampak positif yang signifikan dalam meningkatkan pelayanan publik berbasis sosio-kultural. Hal ini terlihat dari tingginya antusiasme masyarakat dalam mengunduh aplikasi Jogja Smart Service. Lebih lanjut, pembangunan infrastruktur berbasis IT juga telah dirasakan manfaatnya oleh masyarakat, menunjukkan efektivitas dari program tersebut. Pemerintah Kota Yogyakarta, khususnya Dinas Komunikasi, Informasi, dan Persandian, memainkan peran yang sangat aktif dalam memperkuat pelaksanaan konsep smart city di Kota Yogyakarta melalui Jogja Smart Service. Hal ini menunjukkan komitmen mereka dalam meningkatkan kualitas pelayanan publik dan memanfaatkan teknologi untuk kepentingan sosial dan budaya (Wibisono and Handoko, 2020). Layanan yang disediakan oleh pemprov Yogyakarta antara lain (jsp.jogjaprov.go.id, 2020):

1. Lapor online melalui E-Lapor, Pemerintah DIY melalui Dinas Komunikasi dan Informatika telah mengembangkan aplikasi layanan pengaduan publik yang terintegrasi. Aplikasi ini merupakan gabungan dari E-Lapor DIY, App Jogja Istimewa, dan LAPOR SP4N milik Kementerian PANRB RI. Integrasi ini sesuai dengan semangat kolaborasi dan integrasi kewilayahan, yang merupakan program prioritas Gubernur DIY, Jogja Smart Province. Diluncurkannya versi baru E-Lapor DIY yang dapat diakses melalui Jogja Istimewa diharapkan dapat memudahkan masyarakat untuk menyampaikan

laporan, keluhan, dan masukan terkait layanan publik dan pembangunan di DIY, serta memantau respon dan feedback dari Pemerintah DIY. Jogja Istimewa juga merupakan platform aplikasi mobile yang menyediakan informasi dan layanan publik Yogyakarta, tidak hanya untuk masyarakat setempat, tetapi juga untuk wisatawan atau pengunjung.

2. *Smart Environment*, adalah konsep lingkungan yang dikelola secara baik, berkelanjutan, dan efisien dengan memanfaatkan teknologi informasi dan data. Sasaran dari *Smart Environment* termasuk membangun sistem informasi untuk pengelolaan penyediaan air baku secara efisien, meningkatkan kesadaran lingkungan masyarakat, memperbaiki pengelolaan drainase perkotaan, membangun sistem informasi persampahan untuk kebijakan dan edukasi masyarakat, serta memantau volume dan karakteristik air limbah di DIY.
3. *Smart Culture*, konsep yang menggambarkan budaya yang mampu meningkatkan martabat, kesejahteraan, dan kesatuan manusia Jogja dengan Sang Maha Pencipta.
4. *Smart Society* menjadi misi pertama dalam Jogja *Smart Province*. Sasaran dari *Smart Society* meliputi pembangunan sistem pendidikan yang memberikan kesempatan pendidikan yang luas bagi masyarakat, pembangunan masyarakat yang adaptif terhadap perubahan, ekosistem ekonomi yang kreatif, inovatif, dan produktif, serta menciptakan kondisi masyarakat yang aman, damai, ber-Bhinneka Tunggal Ika, hidup bersama dalam keragaman, dan terhindar dari paham radikalisme.
5. *Smart Living* merupakan misi kedua dalam Jogja *Smart Province*. Sasaran dari *Smart Living* mencakup harmonisasi tata ruang wilayah (*harmony*), penyediaan prasarana kesehatan (*health*) yang berkualitas, serta jaminan ketersediaan sarana transportasi (*mobility*) yang aman, efisien, dan terpadu.

9.3.4 Makassar

Dalam penerapan *smart city*, pemrov makassar mewujudkan dalam misi Sombere dan *Smart city* dengan imunitas kota yang kuat untuk semua. Terdapat tiga misi antara lain revolusi sumber daya manusia, rekonstruksi kesehatan, ekonomi, sosial budaya, dan restorasi ruang kota yang inklusif menuju kota nyaman kelas dunia. Perjalanan inisiatif *smart city* kota makassar telah dimulai sejak tahun 2015 melalui komitmen, kolaborasi, integrasi, interopera dan makaverse.

Penyatuan nilai-nilai luhur budaya etnis "Bugis Makassar" yang ramah tamah dan santun dengan pemanfaatan Teknologi Informasi dan Komunikasi (TIK) dalam pelayanan dan pemberdayaan masyarakat serta pembangunan, merupakan upaya menciptakan Makassar sebagai kota cerdas. Konsep "Sombere" mencakup aspek Heartware atau "Perangkat Hati", yang menyoroti nilai-nilai budaya lokal, sementara *Smart City* melibatkan Hardware dan *Software* atau "Perangkat Keras" dan "Perangkat Lunak". Harapannya, integrasi antara Sombere' dan *Smart City* akan membawa Makassar menjadi kota cerdas yang tidak hanya berbasis teknologi, tetapi juga memiliki karakter budaya lokal yang kuat. Komponen *smart city* kota makassar antara lain :

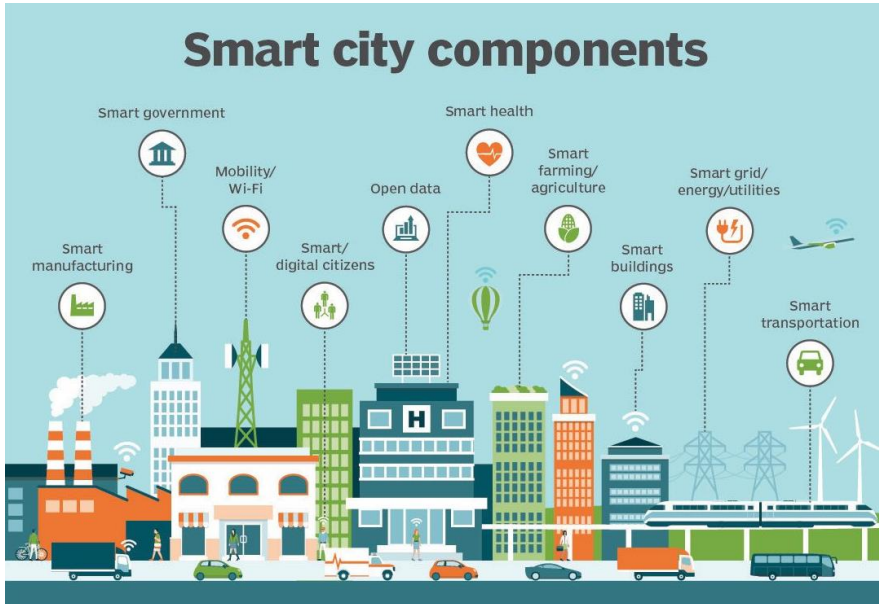
1. *Smart governance*, integrasi pemerintahan, kolaborasi, dan Efisiensi birokrasi (*e-governance* yang efisien)
2. *Smart living*, integrasi tata ruang inklusif, pelayanan publik berkualitas tinggi, dan Sistem transportasi cerdas dengan integrasi multi-modal (transportasi)
3. *Smart economic*, pengembangan ekosistem kreatif berbasis TIK yang kompetitif (industri kreatif), Kesejahteraan, dan Ekosistem transaksi elektronik (transaksi elektronik)
4. *Smart society*, keterlibatan masyarakat, Pembangunan ekosistem literasi tinggi, Penguatan sistem keamanan lingkungan masyarakat (kota yang tangguh)
5. *Smart environment*, perlindungan Lingkungan, Pengelolaan limbah dan sampah, Pemanfaatan energi yang lebih efisien (efisiensi energi).

6. Smart branding, penguatan bisnis inti atau produk unggulan daerah, Pengembangan arsitektur kota yang mencerminkan kearifan lokal (penampilan kota).

9.4 Smart City berbasis IoT

Smart City memanfaatkan infrastruktur IoT yang terkoneksi dan teknologi lainnya guna mencapai tujuannya dalam meningkatkan kualitas hidup serta pertumbuhan ekonomi. *Smart City* berbasis IoT dikatakan berhasil jika mengikuti empat tahap antara lain (Shea, 2020):

1. Pengumpulan Data - Sensor cerdas tersebar di seluruh kota untuk mengumpulkan data secara real-time.
2. Analisis - Data yang terkumpul dari sensor cerdas dianalisis untuk memperoleh pemahaman yang signifikan.
3. Komunikasi - Hasil analisis disampaikan kepada para pengambil keputusan melalui jaringan komunikasi yang handal.
4. Implementasi - Kota menggunakan wawasan yang diperoleh dari data untuk mengembangkan solusi, mengoptimalkan operasional dan manajemen aset, serta meningkatkan kualitas hidup penduduknya.



Gambar 9.2. Komponen smart city

(Sumber:

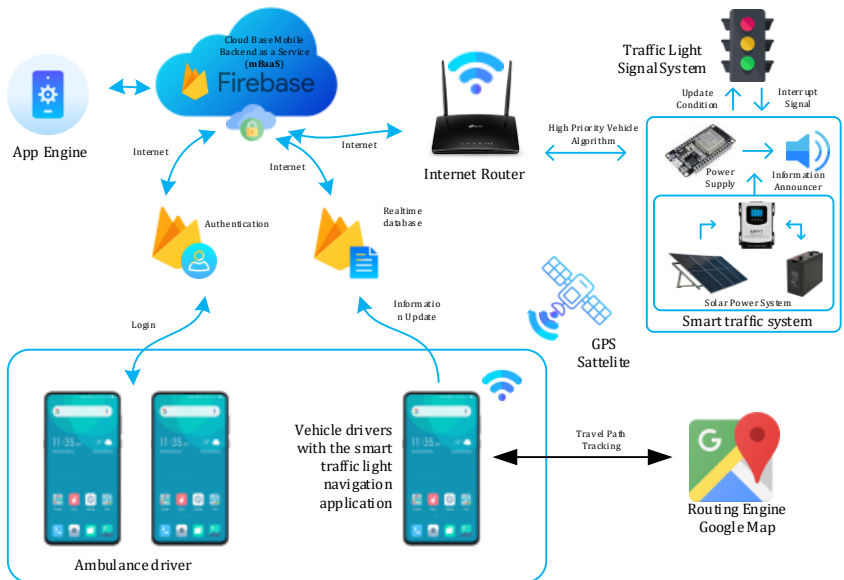
<https://www.techtarget.com/iotagenda/definition/smart-city>)

9.4.1 Smart Traffic Light

Sistem Pengembangan Smart Traffic Light berbasis IoT (*Internet Of Things*) dengan *Mobile Backend as a Service* (MbaaS) adalah bagian dari inisiatif untuk menciptakan *Smart City* dalam bidang Transportasi. Sistem ini, seperti yang ditunjukkan pada Gambar 9.3, menggunakan layanan *Backend Service Firebase* yang mencakup Realtime Database, Authentication, REST Support, Data Analysis, dan *SaaS Service*. Penggunaan layanan Firebase memungkinkan komunikasi antara *Smart Traffic System* dengan pengguna, terutama kendaraan darurat seperti Ambulans yang membutuhkan prioritas saat melintas di jalan raya sesuai dengan Undang-Undang. Komunikasi ini dimungkinkan melalui penggunaan API (*Application Program Interface*). Penggunaan kendaraan berinteraksi dengan sistem *Smart Traffic Light* melalui aplikasi yang terpasang pada smartphone. Aplikasi ini memiliki beberapa fitur utama, termasuk:

1. Login: Untuk mengakses fitur-fitur aplikasi.
2. Routing Jalur: Memberikan rekomendasi jalur yang optimal berdasarkan lalu lintas saat ini.
3. Navigation: Memandu pengguna melalui rute yang telah dipilih.

Aplikasi ini dapat digunakan secara bersama-sama oleh pengguna. Dengan menggunakan GPS yang terdapat di smartphone, aplikasi akan mengirimkan data lokasi kendaraan secara terus-menerus ke Firebase melalui koneksi internet. Hal ini memungkinkan sistem untuk memantau lokasi kendaraan secara *real-time* dan mengoptimalkan aliran lalu lintas berdasarkan informasi tersebut (Bagus and Andraini, 2022).



Gambar 9.3. Desain system smart traffic light

(Sumber:

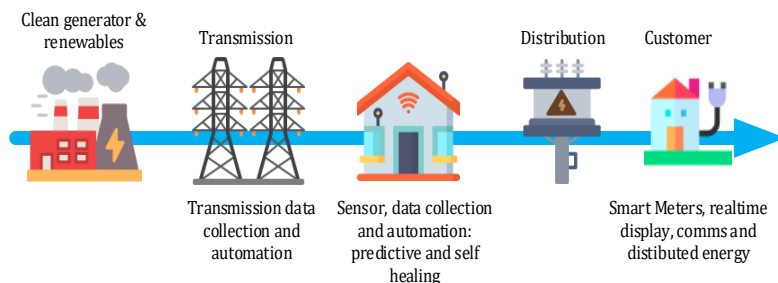
<https://www.techtarget.com/iotagenda/definition/smart-city>)

Sistem *Smart Traffic Light* ini berbasis IoT dan membutuhkan beberapa perangkat untuk mendukung

rancangannya, termasuk ESP8266 yang terhubung ke Firebase melalui koneksi internet. Layanan Firebase yang digunakan pada aplikasi Smart Traffic Light meliputi authentication dan realtime database. Fitur GPS digunakan untuk menyimpan data update lokasi perjalanan ke Firebase melalui koneksi internet. Dengan demikian, ESP8266 berfungsi sebagai penghubung antara sistem *Smart Traffic Light* dan layanan Firebase, sementara GPS digunakan untuk memperbarui data lokasi kendaraan secara terus-menerus (Zulianti, Munadi and Santoso, 2021). Dalam penerapannya, *smart traffic light* ini sangat menunjang konsep smart living pada *smart city*.

9.4.2 Smart Grid

Jaringan listrik cerdas, atau yang lebih dikenal sebagai Smart Grid, merupakan sebuah transformasi teknologi di industri ketenagalistrikan. *Smart Grid* adalah jaringan energi listrik modern yang cerdas, yang mampu mengintegrasikan jaringan listrik dengan perangkat komunikasi yang mendukung pembangkit dan jaringan transmisi distribusi listrik menjadi lebih atraktif, komunikatif, dan berkualitas. Smart Grid juga memiliki kemampuan untuk mencegah dan mengisolasi gangguan dengan cepat, serta menyajikan informasi data kelistrikan *secara real-time*. Secara teknis, IoT dapat memainkan peran penting dalam pengembangan jaringan Smart Grid dengan mengintegrasikan infrastruktur utama sistem kelistrikan mulai dari sisi pembangkit hingga konsumen akhir melalui jaringan sensor nirkabel secara otomatis (Asyik Hidayatullah and Eko Juliando Sudirman, 2017).



Gambar 9.4. Konsep smart grid
(Sumber: Southern California Edison & CPUC)

Smart grid berkaitan erat dengan smart environment dalam konsep *smart city*. Sumber daya energi yang digunakan akan dipantau secara efektif sehingga menjamin pemanfaatan energi yang lebih efisien.

DAFTAR PUSTAKA

- Amalia, D., Nesya, N. and Tyrta, M. (2023) 'Implementasi Kota Pintar (Smart City) Di Kota Surabaya', *Ministrate: Jurnal Birokrasi & Pemerintahan Daerah*, 5(1), pp. 57–63.
- Angelakis, V. *et al.* (eds) (2017) *Designing, Developing, and Facilitating Smart Cities*. Cham: Springer International Publishing. Available at: <https://doi.org/10.1007/978-3-319-44924-1>.
- Arman (2019) 'Smart City: Konsep Kota Pintar Di Dki Jakarta', 20(2), p. 73.
- Asyik Hidayatullah, N. and Eko Juliando Sudirman, D. (2017) 'Desain Dan Aplikasi Internet Of Thing (Iot) Untuk Smart Grid Power System', 2(1), pp. 35–44.
- Bagus, I. and Andraini, L. (2022) 'Pengembangan Smart Traffic Light Berbasis IOT Dengan Mobile Backend As A Service Sebagai Wujud Smart City Bidang Transportasi', *Portaldata.org*, 2(10), pp. 2022–2023.
- jsp.jogjaprovo.go.id (2020) *Jogja Smart Province*, jsp.jogjaprovo.go.id. Available at: <https://jsp.jogjaprovo.go.id/kategori/3> (Accessed: 9 May 2024).
- Puspitasari, C. (2021) *Penerapan Smart City Di Indonesia*. Available at: <https://binus.ac.id/malang/2021/04/penerapan-smart-city-di-indonesia/> (Accessed: 6 May 2024).
- Setiawan, I. and Aindita, E.T.F. (2022) 'Penerapan Konsep Smart City Dalam Tata Kelola Pemerintahan Kota Semarang', *Jurnal Ilmiah Administrasi Pemerintahan Daerah*, 14(1), pp. 97–116. Available at: <https://doi.org/10.33701/jiagd.v14i1>.
- Shea, S. (2020) *Smart City*, www.techtarget.com. Available at: <https://www.techtarget.com/iotagenda/definition/smart-city> (Accessed: 6 May 2024).
- Sofa, A. (2023) *Kenali Smart City, Definisi dan Pengertiannya*, smartcity.jakarta.go.id. Available at: <https://smartcity.jakarta.go.id/id/blog/mengenal-konsep-pengertian-smart-city/> (Accessed: 6 May 2024).

- Wibisono, B.S. and Handoko, S. (2020) 'Program Jogja Smart City dalam Meningkatkan Pelayanan Publik Berbasis Sosio-Kultural', *Jurnal Kewarganegaraan*, 4(1), pp. 66–74.
- Zulianti, F., Munadi, R. and Santoso, I.H. (2021) 'Smart Traffic Light Berbasis Internet Of Things Pada Keselamatan Ambulans Smart Traffic Light Based Internet Of Things On Ambulance Safety', *e-Proceeding of Engineering*, 8(5), pp. 5546–5553.

BAB 10

IMPLEMENTASI IOT PADA PERTANIAN RUMAH JAMUR

Oleh Julianti Habibuddin

10.1 Pendahuluan

10.1.1 Pengertian IoT

IoT, singkatan dari *Internet of Things*, merujuk pada rangkaian perangkat yang terhubung secara nirkabel. Ini memfasilitasi pengumpulan, pemrosesan, dan analisis data untuk memberikan informasi yang bermanfaat kepada pengguna (Fawaz, 2018). *IoT* adalah gagasan yang bertujuan untuk memperluas manfaat dari konektivitas internet yang berkelanjutan, yang memungkinkan berbagai perangkat untuk terus terhubung dan berinteraksi (Danny & Wahyudi, 2018).

IoT adalah infrastruktur yang terdiri dari perangkat fisik, kendaraan, peralatan, dan barang lainnya yang dilengkapi dengan teknologi seperti elektronik, perangkat lunak, sensor, aktuator, dan koneksi jaringan. Ini memungkinkan objek-objek tersebut untuk mengumpulkan dan bertukar data secara otomatis. *IoT* adalah kemampuan suatu objek untuk mentransfer data melalui jaringan tanpa memerlukan interaksi manusia secara langsung, baik antara manusia ke manusia maupun manusia ke komputer (Budihartono et al., 2022).

Internet of Things (IoT) adalah hasil dari evolusi teknologi internet yang memungkinkan setiap objek yang dimiliki untuk terhubung ke internet, memungkinkan pengendalian dari jarak jauh melalui smartphone atau perangkat lainnya (Budiman et al., 2021).

Internet of Things (IoT), atau yang lebih dikenal dengan singkatan *IoT*, bukanlah nama perangkat khusus atau aplikasi tertentu. Sebaliknya, *IoT* merupakan bagian dari teknologi internet yang memungkinkan objek atau kumpulan perangkat untuk saling terhubung dan bertukar data melalui internet tanpa interaksi

langsung manusia atau komputer. Konsep dasar dari *IoT* adalah memanfaatkan internet untuk menciptakan sistem cerdas yang menghubungkan objek atau perangkat secara bersamaan. Objek-objek atau perangkat-perangkat tersebut dapat saling berkomunikasi, bertukar data, dan mengenali satu sama lain tanpa campur tangan manusia (Rusina, 2023).

Sistem *Internet of Things (IoT)* mengintegrasikan dunia fisik dengan Internet. *IoT* berfungsi menghubungkan antarmuka dunia fisik dengan Internet, seperti sensor yang mengumpulkan data dan aktuator yang bertindak berdasarkan kondisi lingkungan disekitarnya. Ini memungkinkan sistem *IoT* untuk menggabungkan teknologi yang menghubungkan sensor dan instrumen, serta memperoleh dan mengirimkan data dari dunia fisik ke Internet. Proses ini mengatasi celah antara dunia fisik dan virtual yang telah ada sejak munculnya komputer. *IoT* membawa fitur dan kemampuan Internet ke dalam dunia nyata. Dengan adopsi *IoT*, Internet menjadi jaringan yang menghubungkan individu, informasi, layanan, bisnis, dan sektor-sektor penting lainnya. Sebagaimana diungkapkan oleh Kevin Ashton, pencipta istilah *Internet of Things* (Erwin et al.,2023).

Pada Bab ini memfokuskan pada pembahasan implementasi *IoT* pada bidang pertanian. Salah satu contohnya adalah penggunaan *IoT* oleh petani jamur dalam mengelola rumah jamur. Tujuannya adalah untuk meningkatkan efisiensi dalam pengaturan suhu dan kelembapan di dalam rumah jamur. Dengan demikian, petani jamur tidak perlu melakukan tugas yang berulang karena beberapa pekerjaan tersebut dapat dilakukan oleh mesin yang terhubung dengan sistem *IoT*.

10.1.2 Rumah Jamur

Rumah jamur, juga dikenal sebagai rumah kumbung, adalah struktur yang sering digunakan untuk menumbuhkan jamur tiram. Bentuk dan dimensi rumah jamur dapat disesuaikan dengan kebutuhan. Sebagai contoh, untuk menampung sekitar 500-1.500 baglog, sebuah bangunan dengan ukuran 6 meter x 4 meter x 4 meter akan diperlukan. Kelembapan adalah salah satu faktor kunci yang memengaruhi pertumbuhan jamur. Oleh karena itu, rumah

jamur yang ideal harus mampu menjaga kelembapan yang dibutuhkan oleh jamur. Seperti yang telah disebutkan sebelumnya, pembuatan rumah jamur dapat memanfaatkan ruang di dalam rumah atau halaman (Yohana, 2010).

Dinding rumah jamur bisa menggunakan berbagai bahan seperti tembok, anyaman bambu, kayu, atau terpal sederhana. Untuk menjaga sirkulasi udara, disarankan untuk memberikan ventilasi yang memadai di bagian atas dinding, dengan dua ventilasi di sisi kanan dan dua di sisi kiri rumah kumbung. Penting untuk memasang kasa di lubang ventilasi tersebut agar hewan seperti burung dan serangga tidak masuk. Lantai rumah jamur sebaiknya pasir atau tanah untuk menjaga kelembapan setelah penyiraman. Atapnya dapat terbuat dari genting, anyaman bambu, atau seng. Biasanya, rumah jamur yang terbuat dari anyaman bambu atau kayu memerlukan rehabilitasi setiap dua tahun, termasuk penggantian material yang sudah tidak layak pakai. Rumah jamur yang terjaga kebersihannya, mengurangi risiko kontaminasi jamur oleh hama dan penyakit. (Yahona, 2010).

Rumah jamur harus memenuhi syarat tumbuh jamur, adapun syarat yang harus dipenuhi adalah : kebersihan kumbung, sirkulasi udara yang baik, suhu dan kelembapan, pencahayaan dan tertutup (Isnaen, 2010).

Lokasi rumah jamur perlu diperhatikan, apabila di daerah dataran rendah suhu udara lingkungan sebesar 30-32 °C untuk jamur merang. Untuk jamur kancing dan jamur shitake diusahakan di daerah dataran tinggi dengan besaran suhu 20-24 °C. Selain itu lokasi budidaya jamur jauh dari pabrik atau pembuangan limbah berbahaya. Lokasi yang dipilih dekat dengan bahan baku dan sumber air yang digunakan (Agriflo, 2012).

10.2 Prinsip Kerja *IoT* pada Rumah Jamur

Teknologi berbasis internet, terdapat beberapa komponen yang digunakan yaitu : Sensor, Koneksi, pengolahan data, User interface dan perangkat pendukung lainnya. Sensor dapat mengumpulkan data berupa besaran fisis kemudian memproses dengan mengubah ke besaran listrik dan mengirikan data tersebut ke mikrokontroller. User interface sebagai mikrokontroller yang

dapat terhubung pada *Platform IoT*. Pemrograman dan pengolahan data (berupa perintah) dilakukan oleh mikrokontroller. Untuk menghubungkan mikrokontroller ke *Platform IoT* dibutuhkan koneksi (konektivitas). Koneksi ini penting untuk menghubungkan antara perangkat atau mesin satu dengan yang lainnya, dan memiliki dampak besar pada proses pengiriman data atau informasi. Tanpa koneksi yang baik, data tidak akan dapat diproses, mengakibatkan mesin atau perangkat tidak dapat saling memberikan instruksi.

Rumah jamur adalah salah satu contoh pada bidang pertanian dalam penerapan teknologi *Internet of Things*. Pengumpulan data suhu dan kelembapan untuk diolah yang kemudian dihasilkan keputusan untuk melakukan penyiraman misalnya untuk menjaga kelembapan pada rumah jamur. Secara umum dibutuhkan sensor untuk mengukur suhu dan kelembapan, mikrokontroller sebagai otak atau pengolah data/program data dan aktuator sebagai perangkat untuk melaksanakan keputusan/tindakan. Pada ruang tersebut harus terkoneksi dengan modem (menghubungkan ke jaringan internet) untuk menghubungkan mikrokontroller ke *Platform IoT*.

10.3 Penerapan *IoT* pada Rumah Jamur

Mesin diciptakan untuk mempermudah pekerjaan manusia. Pada awalnya, mesin dibuat untuk membantu manusia dan dioperasikan secara manual. Seiring waktu, mesin menjadi mampu berjalan sendiri secara otomatis. Namun, dalam perkembangannya, penggunaan mesin sebagai alat dalam sistem akan menghadapi kendala terutama terkait dengan jarak dan waktu. Dengan jarak yang sangat jauh, mesin tidak dapat berinteraksi dengan mesin lainnya. Untuk mengatasi masalah ini, konsep *Internet of Things (IoT)* diterapkan, di mana semua mesin yang memiliki alamat IP dapat menggunakan jaringan internet sebagai media komunikasi untuk bertukar data (Akmal, 2019).

Penerapan *IoT* pada bidang pertanian yang dibahas pada subbab ini adalah penyiraman otomatis pada rumah jamur untuk menjaga suhu dan kelembapan rumah jamur. Penyiraman secara

otomatis dilakukan saat kelembapan rumah jamur terdeteksi dibawah standar.

10.3.1 Monitoring Suhu dan Kelembapan

Monitoring suhu dan kelembapan menggunakan beberapa komponen dan perangkat elektronik. Komponen elektronik yang digunakan adalah sensor temperature dan kelembapan, dapat berupa DHT22. DHT22 adalah sebuah sensor modul yang digunakan untuk mengukur suhu dan kelembapan di dalam suatu ruangan. Sensor ini memiliki 3 pin dengan fungsi yang berbeda. Pin VCC dan Ground berperan sebagai sumber daya untuk memastikan sensor dapat berfungsi secara optimal. Tegangan yang direkomendasikan untuk sensor ini adalah 5 V sesuai dengan datasheet DHT22. Pin sinyal digunakan untuk mengirimkan sinyal analog yang kemudian diolah menggunakan metode ADC (*Analog to Digital Converter*). Dengan menggunakan nilai ADC ini, sensor dapat menampilkan nilai suhu dan kelembapan.

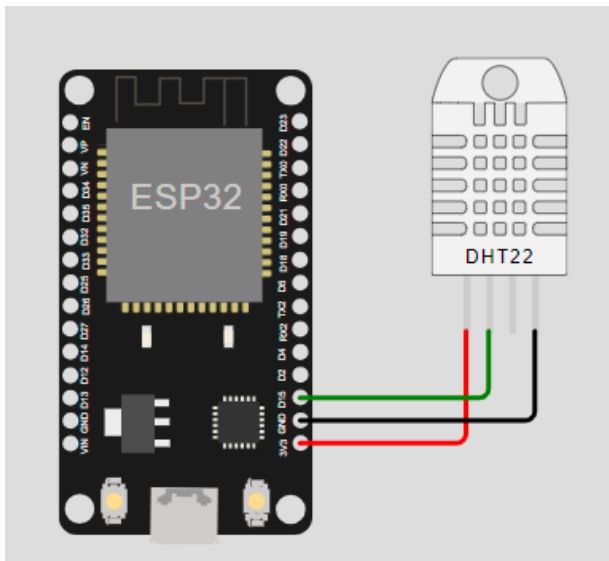
Rangkaian elektronika dapat dibuat pada protoboard (papan simulasi). Selain itu dapat disimulasikan terlebih dahulu pada beberapa aplikasi atau software diantaranya adalah wokwi. Wokwi adalah sebuah *Platform* simulasi elektronika online yang menyediakan berbagai jenis board Arduino, sensor, dan komponen elektronika lainnya yang cukup lengkap untuk mendukung simulasi berbagai proyek. Salah satu keunggulan utamanya adalah adanya dukungan untuk board ESP32, yang memungkinkan pengguna untuk menghubungkan komponen elektronika dengan perangkat online untuk keperluan pemantauan atau monitoring. (Atmoko,R.A., 2023).

Merancang alat monitoring suhu dan kelembapan pada rumah jamur dapat dilakukan secara bertahap yaitu :

1. Persiapan perancangan
2. Mengaktifkan modul ESP32, sensor dan koneksi
3. Mengirimkan nilai ke database

Persiapan perancangan dengan menyiapkan alat dan bahan yang dibutuhkan. Berikut alat dan bahannya : Modul ESP32 Devkit, Sensor DHT22, Breadboard 400 poin, Kabel jumper male to

male, Kabel data micro type dan software Arduino IDE. Persiapan perancangan dapat berupa simulasi menggunakan simulator wokwi. **Mengaktifkan modul ESP32, sensor dan koneksi** menggunakan kode program. Rangkailah sesuai gambar 10.1 kemudian buat kode program program .ino dengan simulasi terhubung ke *Platform IoT* berupa *ThingSpeak*. Berikut gambar rangkaian beserta kode program yang digunakan :



Gambar 10.1. Rangkaian Monitoring Temperatur dan Kelembapan

Kode program :

```
#include "WiFi.h"
```

```
WiFiClient client;
```

```
#include "DHTesp.h"
```

```
const int DHT_PIN = 15;
```

```
DHTesp dhtSensor;;
```

```
String ThingSpeakAddress = "api.ThingSpeak.com";
```

```

String writeAPIKey;
String tsfield1Name;
String request_string;
void setup()
{
  Serial.begin(9600);
  WiFi.disconnect();
  WiFi.begin("Wokwi-GUEST", "");
  while ((!(WiFi.status() == WL_CONNECTED))) {
    delay(300);
    Serial.print(".");
  }
  Serial.println("");
  Serial.println("WiFi connected");
  Serial.println("IP address: ");
  Serial.println(WiFi.localIP());
  dhtSensor.setup(DHT_PIN, DHTesp::DHT22);
}
void loop()
{
  delay(2000);
  TempAndHumidity data = dhtSensor.getTempAndHumidity();

  float t = data.temperature;
  float h = data.humidity;

  kirim_ThingSpeak(t, h);

  if (isnan(h) || isnan(t) ) {
    Serial.println("Failed to read from DHT sensor!");
    return;
  }
}

void kirim_ThingSpeak(float suhu, float hum) {
  if (client.connect("api.ThingSpeak.com", 80)) {
    request_string = "/update?";
    request_string += "key=";
  }
}

```

```

request_string += "9HQRUABN28VP5DS7";
request_string += "&";
request_string += "field1";
request_string += "=";
request_string += suhu;
request_string += "&";
request_string += "field2";
request_string += "=";
request_string += hum;

    Serial.println(String("GET  ") + request_string + "
HTTP/1.1\r\n" +
        "Host: " + ThingSpeakAddress + "\r\n" +
        "Connection: close\r\n\r\n");

client.print(String("GET ") + request_string + " HTTP/1.1\r\n"
+
    "Host: " + ThingSpeakAddress + "\r\n" +
    "Connection: close\r\n\r\n");
unsigned long timeout = millis();
while (client.available() == 0) {
    if (millis() - timeout > 5000) {
        Serial.println(">>> Client Timeout !");
        client.stop();
        return;
    }
}

while (client.available()) {
    String line = client.readStringUntil('\r');
    Serial.print(line);
}
Serial.println();
Serial.println("closing connection");
}
}

```

Adapun diagram json dapat dilihat pada gambar dibawah ini :

```
1 {
2   "version": 1,
3   "author": "Anonymous maker",
4   "editor": "wokwi",
5   "parts": [
6     { "type": "wokwi-esp32-devkit-v1", "id": "esp", "top": 0, "left": 0, "attrs": {} },
7     { "type": "wokwi-dht22", "id": "dht1", "top": -3.37, "left": 155.83, "attrs": {} }
8   ],
9   "connections": [
10    [ "esp:TX0", "$serialMonitor:RX", "", [] ],
11    [ "esp:RX0", "$serialMonitor:TX", "", [] ],
12    [ "dht1:VCC", "esp:3V3", "red", [ "v0" ] ],
13    [ "dht1:SDA", "esp:D15", "green", [ "v0" ] ],
14    [ "dht1:GND", "esp:GND.1", "black", [ "v0" ] ]
15  ]
16 }
```

Gambar 10.2. Coding diagram json monitoring temperatur dan kelembapan

Mengirim nilai ke database membutuhkan inisialisasi alamat server untuk disambungkan ke database (Atmoko,R.A., 2023).

Monitoring temperatur dan kelembapan pada rumah jamur penting bagi petani jamur. Dengan memasang alat pemantau suhu dan kelembapan di rumah jamur, besaran fisis dapat diukur dengan akurat. Sebagian besar petani jamur hanya membuat perkiraan tentang temperatur dan kelembapan saat mengecek rumah jamur untuk dilakukan penyiraman. Dengan adanya alat pemantauan temperatur dan kelembapan petani jamur tidak perlu datang ke rumah jamur untuk memantau nilai temperatur dan kelembapan rumah jamur, cukup dengan memantau via smartphone. Adapun salah satu *Platform IoT* yang dapat digunakan untuk memantau temperatur dan kelembapan rumah jamur adalah *Platform ThingSpeak*.

10.3.2 Penyiraman Otomatis

Penyiraman adalah rutinitas yang sangat penting dalam pemeliharaan tanaman agar tetap hidup dan berkembang. Sistem penyiraman otomatis dapat mengurangi beban kerja dengan menyediakan air secara otomatis saat tanaman membutuhkannya.

Otomatisasi dapat menjadi solusi untuk menjalankan tugas-tugas rutin karena dapat beroperasi secara terus-menerus tanpa memperhatikan waktu. Mengetahui kapan penyiraman perlu dilakukan merupakan aspek kunci dari proses penyiraman. Sistem ini diprogram untuk mendeteksi tingkat kelembaban tanaman jamur tiram dan memberikan air jika diperlukan. Sistem ini umumnya digunakan untuk merawat tanaman secara umum, terkhusus dalam merawat rumah jamur. Sistem Penyiraman Otomatis Berbasis Mikrokontroller ESP32 memiliki potensi untuk meningkatkan efisiensi suatu organisasi atau IKM (Industri Kecil Menengah) dalam sektor pertanian atau perkebunan. Jika penyiraman tanaman jamur dapat dilakukan secara otomatis dengan bantuan alat, ini sangat menguntungkan dan mempermudah proses perawatan tanaman jamur. (Budihartono et al.,2023).

Pada penyiraman otomatis pada rumah jamur rangkaian yang digunakan sama dengan rangkaian yang digunakan pada monitoring temperatur dan kelembapan yaitu sensor DHT22, ESP32 dan *Platform IoT* berupa *ThingSpeak*. Perbedaannya hanya pada keluaran (*Output*). Pada penyiraman otomatis menambahkan output berupa aktuator (pompa dan sprinkle yang terhubung dengan sumber air untuk proses penyiraman). Adapun prinsip kerjanya : ESP32 diprogram pada nilai kelembapan tertentu, misalnya dibawah 85%, maka pompa aktif untuk proses penyiraman untuk menjaga kelembapan rumah jamur. Apabila sensor DHT22 mendeteksi kelembapan 85% atau lebih maka pompa off (berhenti menyiram).

DAFTAR PUSTAKA

- Ade Putra, dkk. 2023. Pemanfaatan Dan Penerapan *Internet of Things (IoT)* Di Berbagai Bidang. Jambi: PT. Sonpedia Publishing Indonesia.
- Erwin, dkk. 2023. Pengantar & Penerapan *Internet of Things* (Konsep dasar & Penerapan *IoT* di berbagai Sektor). Jambi: PT. Sonpedia Publishing Indonesia.
- Yohana, dkk. 2010. Usaha 6 Jenis Jamur Skala Rumah Tangga. Jamur. Jakarta: PT Niaga Swadaya.
- Isnaen Wiardani. 2010. Budi daya Jamur Konsumsi. Yogyakarta : Lili Publisher.
- Tim Penulis Agriflo. 2012. Jamur. Depok, Indonesia: Penebar Swadaya Grup.
- Akmal. 2019. Lebih dekat dengan Industri 4.0. Yogyakarta: Deepublish.
- Zen Munawar. 2022. Fundamental *Internet of Things (IoT)*. Bandung: Kaizen Media Publishing.
- Atmoko, R.A.,. 2023. Berlatih Membuat Proyek Berbasis *Internet of Things*. Penerbit: Filosofis Indonesia Press
- Setiawardhana. 2021. 14 Jam Belajar Cepat *Internet of Things (IoT)*. Yogyakarta: Deepublish
- Pratiwi, dkk. Usaha Jamur Tiram. Niaga Swadaya.
- Afrizal, dkk. 2023. *Internet of Things*. Jawa Barat: Penerbit Adab CV. Adanu Abimata
- Budihartono, dkk. 2023. Sistem Monitoring Dan Penyiraman Otomatis Pada Budidaya Porang Berbasis *IoT*. Penerbit: NEM

BAB 11

IMPLEMENTASI IOT PADA KESEHATAN

Oleh Muhammad Sainal Abidin

11.1 Pendahuluan

Saat ini terjadi perkembangan yang sangat pesat pada bidang teknologi. Teknologi yang berkembang begitu pesat terjadi di semua aspek termasuk pada bidang internet. Internet yang sebelumnya hanya digunakan manusia sebagai akses dalam bertukar informasi, saat ini pemanfaatannya menjadi lebih luas. Salah satu perkembangan yang terjadi pada bidang internet adalah adanya metode yang disebut dengan IoT (*Internet of Things*) yang dapat menghubungkan antara manusia sebagai pengguna dan suatu alat ataupun antar sesama peralatan tanpa terkendala jarak (Fitriawan dkk., 2020). Dengan demikian metode IoT ini sudah mulai diterapkan pada beberapa bidang pekerjaan seperti industri, transportasi dan kesehatan (Sukmadilaga & Rosadi, 2020).

Pada bidang kesehatan, penerapan IoT sudah mulai banyak dijumpai pada beberapa pelayanan kesehatan. Dengan adanya metode IoT yang diterapkan, maka akan meningkatkan kualitas dari pelayan kesehatan tersebut. Proses-proses yang sebelumnya dilakukan secara manual dan sangat bergantung pada peran manusia sebagai operator sudah mulai ditinggalkan dan beralih pada sistem yang elektronik dan otomatis. Penerapan IoT sebenarnya telah dilakukan sejak lama, namun perkembangan mulai sangat terlihat pada saat terjadi wabah covid-19. Dimasa pandemi tersebut terjadi perubahan pola interaksi antar manusia untuk mengurangi penularan. Masyarakat dihimbau untuk mengurangi aktifitas di luar rumah bahkan untuk berkerja pun tetap dilakukan di rumah yang kemudian dikenal dengan istilah *Work From Home (WFH)*. Permasalahan ini menyebabkan metode IoT menjadi lebih terkenal dan berkembang. Berbagai pihak berlomba-

lomba untuk mengembangkan teknologi berbasis IoT untuk menunjang pelayanan kesehatan tanpa adanya interaksi langsung antara pasien dengan petugas kesehatan serta dapat dilakukan meskipun pasien tetap berada di rumah. Berikut adalah penjelasan beberapa penerapan IoT dalam bidang kesehatan.

11.2 Pemantauan kesehatan

Seorang pasien yang sedang dirawat pada suatu fasilitas Kesehatan seperti rumah sakit ataupun puskesmas, maka sinyal vitalnya harus senantiasa terpantau dengan baik terlebih lagi jika pasien dalam kondisi kritis. Sinyal vital yang dimaksud seperti suhu tubuh, detak jantung, saturasi oksigen (SPO₂), respirasi dan tekanan darah. Metode sederhana yang dapat digunakan dalam melakukan pemantauan tersebut adalah dengan memasang suatu alat yang dapat mengukur sinyal-sinyal vital tersebut dan petugas Kesehatan (perawat) melakukan pengecekan pada hasil pengukuran secara berkala. Namun dengan metode ini memiliki banyak kekurangan yang menjadikannya tidak efektif. Hal ini terjadi karena perawat harus senantiasa melakukan pengecekan secara berkala yang akan banyak membuang waktu. Selain itu, pengecekan yang dilakukan secara manual dapat berpotensi terjadinya kesalahan saat petugas lalai karena sedang melakukan pekerjaan lain sehingga dapat berakibat fatal pada pasien. Oleh karena itu, maka peralatan yang digunakan untuk melakukan pemantauan dapat dilengkapi dengan sistem IoT (Praveen dkk., 2023). Dengan ada sistem IoT pada alat pemantau kondisi Kesehatan, maka kondisi vital pasien dapat dikirim pada perangkat lain seperti komputer atau *smartphone* secara *real time*. Dengan metode ini juga dapat memberikan peringatan pada petugas jika terjadi ketidaksesuaian pengukuran pada pasien dengan nilai yang seharusnya. Penerapan IoT ini dapat diterapkan secara terpisah pada masing-masing peralatan seperti pada thermometer, pulse oxymetri, tensimeter, dan respirasi pernapasan maupun pada satu alat kompleks seperti pasien monitor yang terlihat pada Gambar 11.13.



Gambar 11.13. Pasien Monitor

Sebagai contoh untuk penerapan pada alat pulse oxymetri yang digunakan untuk mengukur detak jantung dan SPO_2 . Secara umum, pulse oxymetri yang banyak digunakan adalah alat kecil berbentuk seperti penjepit yang dipasangkan pada jari tangan pasien (Gambar 11.14).



Gambar 11.14. Pulse Oxymetri

Salah satu penelitian yang mengembangkan pulse oxymetri berbasis IoT dilakukan oleh Sutiari dkk., 2023. Pada alat ini mengkombinasikan beberapa komponen elektronika, sensor pulse oxymetri berupa modul Max30100 (Gambar 11.14) dan mikrokontroler Esp8266 (Gambar 11.16) sehingga diperoleh suatu alat pulse oxymetri berbasis IoT.

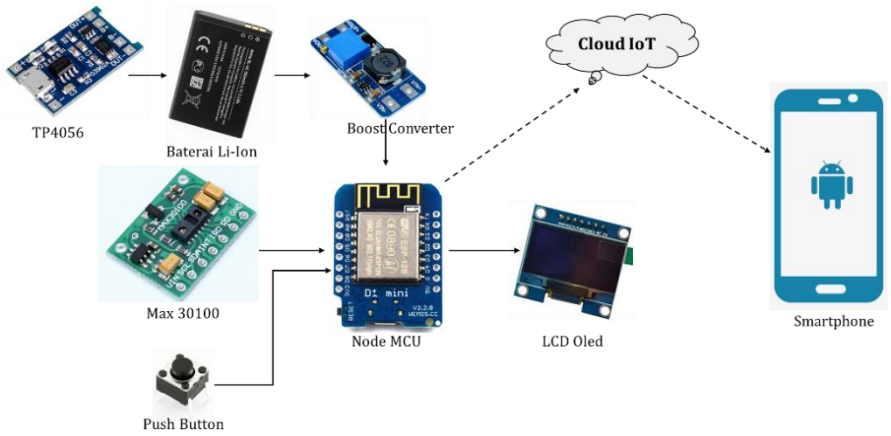


Gambar 11.15. Max30100



Gambar 11.16. Wemos R1 mini Esp8266

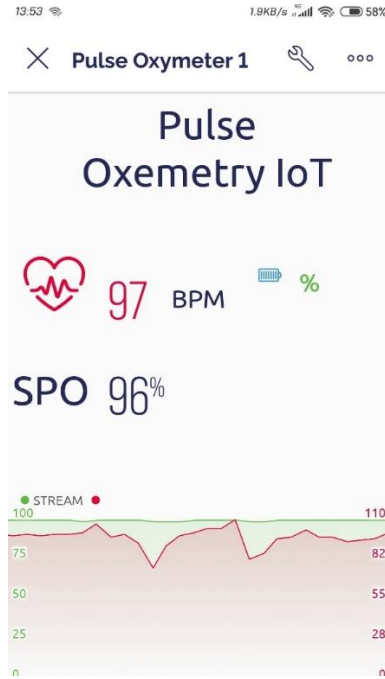
Gambar 11.17 Adalah blok diagram dari alat pulse oxymetri berbasis IoT dengan hasil pengukuran terkirim secara *real time* dan ditampilkan pada *smartphone*. Perancangan alat ini menghasilkan alat pulse oxymetri yang dapat melakukan pengukuran detak jantung dan SPO_2 yang tertampil pada *smartphone* menggunakan aplikasi blynk (Gambar 11.18 dan Gambar 11.19).



Gambar 11.17. Blok diagram pulse Oxymetri berbasis IoT



Gambar 11.18. Alat pulse Oxymetri berbasis IoT



Gambar 11.19. Tampilan Hasil Pengukuran Pada Smartphone

Dengan adanya alat ini, maka pemantauan detak jantung dan saturasi oksigen pasien dapat dilakukan tanpa harus dilakukan pengecekan secara langsung. Hasil pengukuran dari pulse oxymetri ini akan terkirim pada smartphone petugas dan akan memberikan peringatan jika hasil pengukuran melewati ambang batas yang diperbolehkan.

Selain untuk melakukan pemantauan langsung pada manusia, IoT juga dapat diterapkan sistem suatu alat yang tidak berhubungan langsung pada manusia namun akan berdampak pada kesehatan. Pemantauan yang dimaksud seperti pemantauan cairan infus yang diberikan pada pasien. Sebagaimana yang diketahui, pemberian infus dilakukan secara perlahan-lahan dengan volume yang telah ditetapkan. Selain itu, level cairan botol infus juga haruslah terpantau untuk mencegah botol infus yang terlambat diganti karena habis serta berbagai permasalahan yang mungkin terjadi seperti aliran tetesan infus dan selang yang tersumbat. Alat

yang umum digunakan untuk melakukan pengontrolan pemberian infus dikenal dengan nama *Infus Pump* (Gambar 11.20).



Gambar 11.20. Infus Pump

Dengan adanya sistem IoT, maka pemantauan infus dapat langsung terlihat pada smartphone ataupun komputer. Gambar 11.21 memperlihatkan alat monitoring cairan infus berbasis IoT.

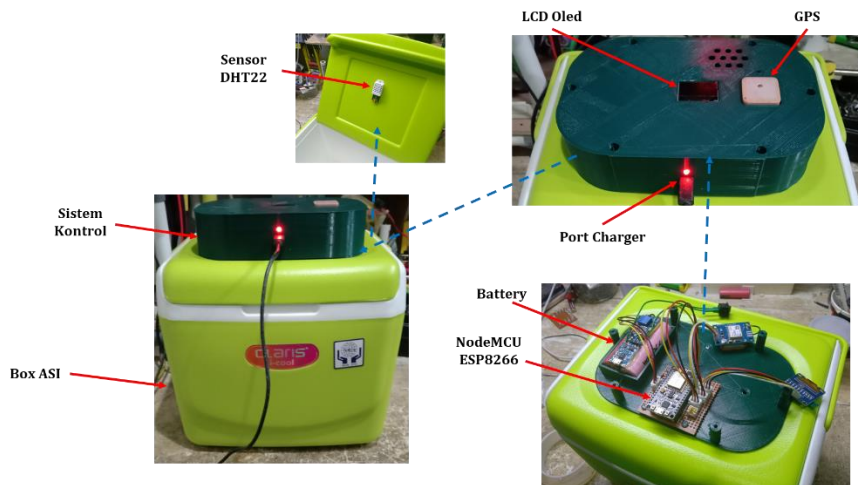


Gambar 11.21. Monitoring unfus berbasis IoT

Alat yang dikembangkan ini dapat melakukan pemantauan volume dan kecepatan tetesan dari sebuah infus yang memanfaatkan sensor berat load cell untuk mengukur berat botol infus dan sensor cahaya untuk memantau tetesan cairan infus (Riyansyah dkk., 2021) (Rosyady dkk., 2023).

Terdapat alat pemantau lain yang dapat dikembangkan berbasis IoT seperti pada alat pemantauan distribusi ASI (Air Susu

Ibu) berbasis IoT yang penelitiannya telah dilakukan oleh Muhammad Sainal Abidin, 2022. Gambar 11.21 merupakan tempat penyimpanan boot ASI yang telah dilengkapi dengan IoT.

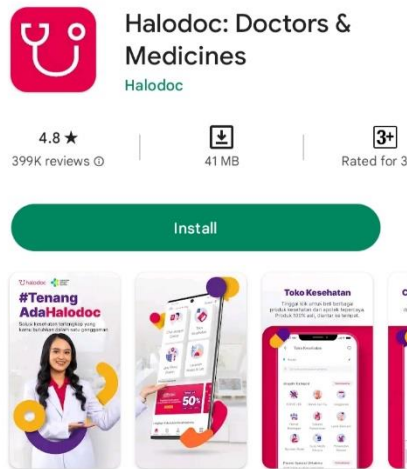


Alat ini bertujuan untuk melakukan pemantauan suhu dan kelembapan wadah penyimpanan botol ASI yang akan distribusikan serta terdapat GPS (*Global Positioning System*) untuk mengetahui lokasi alat. Data suhu, kelembapan serta lokasi dapat terpantau secara langsung pada *Smartphone*. Dengan demikian, kualitas ASI yang akan dikonsumsi oleh bayi dapat terjaga dengan baik.

11.3 Telemedicine

Telemedicine merupakan istilah yang digunakan dalam proses perawatan kesehatan secara jarak jauh. Dengan metode ini memungkinkan dilakukannya perawatan kesehatan pada pasien tanpa harus bertemu langsung dengan petugas kesehatan ataupun mendatangi fasilitas kesehatan. Dalam proses telemedicine dapat menggunakan audio, visual, data, diagnosis, konseling dan diskusi ilmiah seputar kesehatan secara jarak jauh. Untuk dapat menerapkan metode ini, maka tentunya dibutuhkan suatu perangkat pendukung baik perangkat yang sifatnya umum maupun perangkat yang khusus dibuat untuk telemedicine. Perangkat umum yang biasa digunakan seperti *smartphone* yang telah dilengkapi

dengan aplikasi yang dapat menghubungkan pasien dengan petugas kesehatan. Terdapat berbagai macam aplikasi yang dapat diperoleh secara gratis untuk dapat melakukan konsultasi kesehatan. Salah satu aplikasi tersebut adalah aplikasi halodoc seperti yang terlihat pada Gambar 11.22



Gambar 11.22. Aplikasi Halodoc

Namun dengan metode ini pasien hanya sebatas melakukan komunikasi/konsultasi terhadap keluhan yang dialami dengan data/informasi kesehatan diperoleh dengan melakukan pengukuran/pemeriksaan secara terpisah.

11.4 Rekam Medis

Untuk mendukung pelayanan kesehatan, data-data yang telah diperoleh baik itu berupa identitas pasien, hasil pengukuran, pemeriksaan dan tindakan medis yang pernah dialami oleh pasien haruslah tercatat dengan baik. Kumpulan data ini kemudian dikenal dengan istilah rekam medis (Setiawan dkk., 2020). Dengan adanya data rekam medis maka akan mempermudah proses pemberian pelayanan kepada pasien. Data rekam medis yang selama ini dilakukan adalah dengan metode pencatatan manual. Dengan demikian, data rekam medis tersebut hanya dapat diperoleh pada

fasilitas kesehatan yang pernah digunakan oleh pasien dan harus dilakukan pencatatan ulang jika menggunakan fasilitas kesehatan yang berbeda. Dengan adanya sistem IoT yang memungkinkan pertukaran data secara global. Hal ini tentunya dapat diterapkan pada proses rekam medis. Dengan adanya sistem rekam medis yang berbasis IoT, maka data seseorang dapat dengan mudah tersimpan pada komputer untuk dapat akses oleh pihak-pihak yang berwenang dari berbagai tempat. Metode pencarian data juga tidak lagi dilakukan secara manual namun dapat menggunakan sumber pencatatan identitas seperti kartu khusus dan *Finger Print* (sidik jari).

Terdapat beberapa pengembangan sistem untuk melakukan pencatatan rekam medis seperti yang dilakukan oleh Mazed, Nasir dan Anwar, 2019 yang memanfaatkan kartu RFID (*Radio Frequency Identification*) (Mazed dkk., 2019). Dengan adanya sistem pencatatan berbasis elektronik, maka data pasien yang akan menjalani pemeriksaan dapat diakses dan terekam saat kartu RFID discan pada fasilitas kesehatan yang dikunjungi (Musfirah Putri Lukman & Husni Angriani, 2018). Gambar 23.11 adalah topologi rekam medik yang digunakan berbasis IoT dengan menggunakan kartu RFID.



Gambar 23.11. Topologi Rekam Medis Berbasis IoT

Penggunaan kartu RFID sebagai medis mencatatkan rekam medis masih dianggap kurang efektif karena masih berpotensi kartu hilang, lupa dibawa, dan rusak. Dengan demikian terdapat metode pencatatan dengan menggunakan sidik jari sebagai identitas pasien. Gambar 11.24 merupakan contoh penerapan rekam medis menggunakan sidik jari.



Gambar 11.24. Rekam Medis Dengan Sidik Jari

Dengan sistem berbasis sidik jari, maka seorang pasien cukup datang pada fasilitas kesehatan tanpa harus membawa kelengkapan khusus karena sumber identitas bersumber dari sidik jari yang telah didaftarkan sebelumnya. Sebagaimana yang diketahui, sidik jari merupakan bagian dari anggota tubuh yang berbeda untuk setiap manusia (Zaini & Kadafi Nasution, 2021). Sistem yang telah terintegrasi dengan internet akan memudahkan dalam mengakses data rekam medis pasien saat datang pada suatu fasilitas kesehatan. Dengan demikian petugas tidak lagi direpotkan dalam proses mencatat dan mencari data pasien karena akan secara otomatis terakses saat pasien melakukan *scan* sidik jari.

DAFTAR PUSTAKA

- Fitriawan, H., Despa, D., & Kustiani, I. (2020). Potensi Internet of Things (IoT) dan Ragam Sensor untuk Layanan Kesehatan. *Jurnal Profesi Insinyur Universitas Lampung*, 1(1), 1–4. <https://doi.org/10.23960/jpi.v1n1.10>
- Mazed, D., Nasir, M., & Anwar. (2019). Perancangan Sistem Rekam Medis Rumah Sakit Menggunakan RFID Berbasis Internet Of Things. *Jurnal Teknologi Rekayasa Informasi dan Komputer*, 3(1), 1–9.
- Muhammad Sainal Abidin, L. S. Z. (2022). *Rancang Bangun Sistem Pemantauan Distribusi Box Air Susu Ibu (ASI) Berbasis IoT*.
- Musfirah Putri Lukman, & Husni Angriani. (2018). Implementasi Teknologi Rfid Pada Sistem Antrian Rekam Medis Pasien Di Rumah Sakit. *ILKOM Jurnal Ilmiah*, Volume 10(April), 105–112.
- Praveen, B. M., Venkatesh Murthy, B. S., Rajesh Bhat, U., Mallikarjuna, M., Anandraj, R. S., & Bairwa, B. (2023). Real Time Health Monitoring System Using IoT. *2023 IEEE Renewable Energy and Sustainable E-Mobility Conference, RESEM 2023*, 9(4), 515–519. <https://doi.org/10.1109/RESEM57584.2023.10236214>
- Riyansyah, R. G., Wahiddin, D., & Kusumaningrum, D. S. (2021). Smart Monitoring Alat Infus Pasien Berbasis Internet Of Things (IoT) Menggunakan Mikrokontroler ESP32. *Scientific Student Journal for Information, Technology and Science*, 2(2), 142–148. <https://journal.ubpkarawang.ac.id/mahasiswa/index.php/sj/article/view/237>
- Rosyady, P. A., Sukarjiana, A. S. S., Habibah, N. U., Ihsana, N., Baswara, A. R. C., & Dinata, W. R. (2023). Monitoring Cairan Infus Menggunakan Load Cell Berbasis Internet of Things (IoT). *Techné: Jurnal Ilmiah Elektroteknika*, 22(1), 97–110. <https://doi.org/10.31358/techne.v22i1.345>
- Setiawan, E. P., Bhawiyuga, A., & Siregar, R. A. (2020). Pengembangan Sistem Rekam Medis Rumah Sakit dengan Multi User Rest Server berbasis Permissioned Blockchain

- menggunakan Framework Hyperledger. *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer; Vol 4 No 1 (2020)*, 4(1), 1–10. <https://j-ptiik.ub.ac.id/index.php/j-ptiik/article/view/6851>
- Sukmadilaga, A., & Rosadi, S. D. (2020). Upaya Hukum Terhadap Pelanggaran Implementasi Internet Of Things (Iot) Dibidang Pelayanan Kesehatan Menurut Ketentuan Perlindungan Data Pribadi. *Jurnal Suara Keadilan*, 21(2), 205–221. <https://doi.org/10.24176/sk.v21i2.5694>
- Sutiari, D. K., Zulfadlih, L. S., Abidin, M. S., Somayasa, W., & Kizhara, R. (2023). Design SPO2 and BPM Monitoring System To Monitor The Patient's Health Using Anroid. *Indonesian Journal of Health Sciences Research and Development (Ijhsrd)*, 5(1), 42–47. <https://doi.org/10.36566/ijhsrd/vol5.iss1/145>
- Zaini, T., & Kadafi Nasution, M. I. (2021). Sistem Informasi Rekam Medis Berbasis Web Menggunakan Teknologi Sidik Jari (Studi Kasus Puskesmas Kampung Sawah) Bandar Lampung. *SIMADA (Jurnal Sistem Informasi dan Manajemen Basis Data)*, 4(1), 69–78. <https://doi.org/10.30873/simada.v4i1.2743>

BAB 12

IOT DALAM BIDANG LINGKUNGAN

Oleh Tino Suhaebri

12.1 Ruang Lingkup

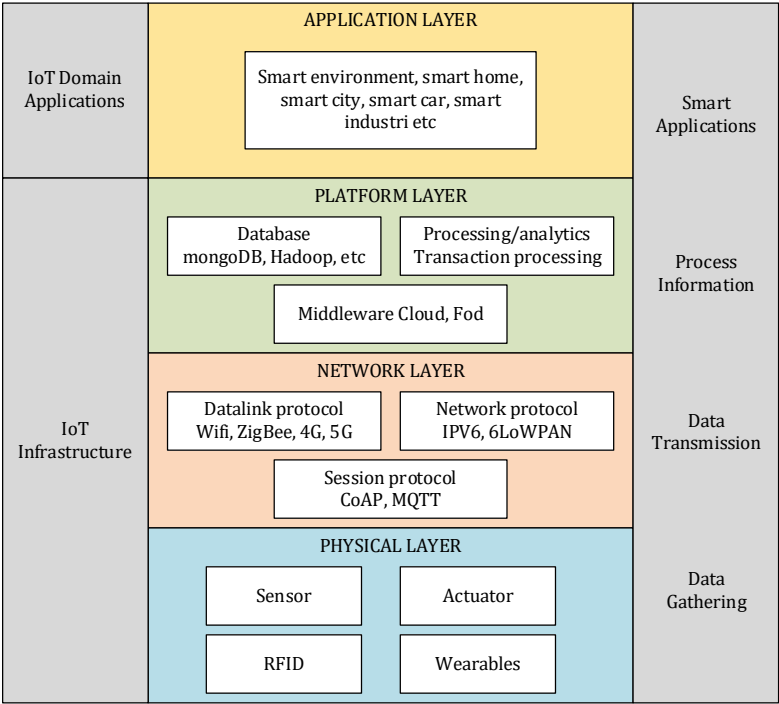
Pemantauan lingkungan melalui *Internet of Things* (IoT) memegang peranan penting dalam memahami dan mengelola dampak lingkungan. Dengan menggunakan sensor dan teknologi terhubung lainnya, pengguna dapat mengumpulkan data secara *real-time* tentang berbagai aspek lingkungan seperti kualitas udara, suhu, dan kelembapan. Data ini kemudian dapat dianalisis untuk mendapatkan wawasan yang lebih baik tentang kondisi lingkungan dan potensi dampaknya.

Salah satu keunggulan utama dari sistem pemantauan lingkungan berbasis IoT adalah kemampuannya untuk mendeteksi masalah lingkungan secara cepat dan akurat. Misalnya, sensor kualitas udara dapat memberi peringatan dini tentang peningkatan polusi udara, sehingga pihak berwenang dapat mengambil tindakan yang diperlukan dalam melindungi kesejahteraan dan kehidupan masyarakat.

Selain itu, data yang dikumpulkan oleh sistem pemantauan lingkungan dapat digunakan untuk mengidentifikasi tren jangka panjang dan pola perilaku lingkungan. Hal ini dapat dimanfaatkan untuk mengambil tindakan dan keputusan yang tepat untuk mengurangi dampak lingkungan dari kegiatan yang dilakukan. Misalnya, analisis data dapat membantu pengguna mengidentifikasi area di mana mereka dapat mengurangi konsumsi energi atau memperbaiki efisiensi penggunaan sumber daya alam lainnya.

Secara keseluruhan, pemantauan lingkungan berbasis IoT adalah alat yang kuat untuk membantu manusia memahami dan mengelola dampak lingkungan dari aktivitas mereka. Dengan menggunakan data yang dikumpulkan oleh sistem, masyarakat dapat mengambil langkah-langkah proaktif untuk melindungi

lingkungan dan mematuhi standar perlindungan lingkungan yang ketat (caburntelecom.com, 2024).



Gambar 12.1. Arsitektur IoT pada Lingkungan Cerdas
(Sumber : (Ikrisi and Mazri, 2021))

Salah satu tujuan utama dari lingkungan cerdas adalah meningkatkan kualitas hidup manusia melalui peningkatan kenyamanan dan efisiensi. Paradigma IoT telah menjadi kunci dalam membangun dan mengembangkan berbagai lingkungan cerdas, seperti kota cerdas, rumah cerdas, kampus cerdas, sistem kesehatan cerdas, dan banyak lagi. Dengan menggunakan teknologi IoT, hal-hal di lingkungan cerdas dapat diotomatisasi dan dihubungkan dalam jaringan, memungkinkan berbagai layanan yang inovatif dan efisien. Contohnya meliputi (Ikrisi and Mazri, 2021):

1. Identifikasi Cerdas: Teknologi IoT memungkinkan identifikasi dan pengenalan otomatis, misalnya, melalui penggunaan

sensor pengenalan wajah atau sensor identifikasi kendaraan. Hal ini dapat membantu meningkatkan keamanan dan efisiensi dalam berbagai konteks, seperti kontrol akses atau pengelolaan parkir.

2. Pemantauan dan Pelacakan: Sensor IoT dapat digunakan untuk memantau berbagai parameter, seperti kualitas udara, suhu, kelembapan, dan lain-lain. Data ini dapat memberikan wawasan yang berharga untuk pengambilan keputusan yang lebih baik dalam manajemen lingkungan.
3. Otomatisasi: Dengan IoT, banyak proses dapat diotomatisasi untuk meningkatkan efisiensi dan kenyamanan. Misalnya, dalam rumah cerdas, sistem otomatisasi rumah dapat mengontrol pencahayaan, pendingin udara, dan perangkat lainnya berdasarkan preferensi dan jadwal penghuni.
4. Manajemen Data: IoT memungkinkan pengumpulan dan analisis data yang besar dan kompleks. Ini dapat digunakan untuk memberikan wawasan yang lebih baik tentang pola perilaku dan kebutuhan pengguna, yang kemudian dapat digunakan untuk mengoptimalkan berbagai layanan.
5. Energi Hijau: Dengan menggunakan sensor IoT dan sistem manajemen energi cerdas, energi dapat dihemat dan digunakan secara lebih efisien, berkontribusi pada upaya untuk mempromosikan energi hijau dan berkelanjutan.

Dengan memanfaatkan potensi teknologi IoT, lingkungan cerdas dapat memberikan manfaat yang signifikan bagi masyarakat, termasuk meningkatkan kenyamanan, efisiensi, keamanan, dan keberlanjutan. Ini menjadikan IoT sebagai salah satu kunci utama dalam membangun masa depan yang lebih cerdas dan berkelanjutan.

Gambar 12.2 menunjukkan bahwa lingkungan cerdas terbentuk dari berbagai domain aplikasi yang saling terkait dan berperan penting. Berikut adalah kategori utama yang mungkin termasuk di dalamnya:

1. Kota cerdas: melibatkan penerapan teknologi cerdas dalam manajemen kota untuk meningkatkan efisiensi, kenyamanan, dan keberlanjutan. Termasuk diantaranya sistem

- transportasi publik yang terhubung, pencahayaan jalan yang terotomatisasi, manajemen limbah yang cerdas, dan lain-lain.
2. Rumah Cerdas: Ini mencakup penggunaan teknologi cerdas dalam rumah tangga untuk meningkatkan kenyamanan, keamanan, dan efisiensi energi. Contohnya termasuk sistem otomatisasi rumah, pengontrol suhu cerdas, pengunci pintu cerdas, dan lain-lain.
 3. Jaringan listrik Cerdas: Ini melibatkan infrastruktur jaringan yang cerdas dan terhubung untuk mendukung berbagai aplikasi IoT. Ini termasuk jaringan sensor, jaringan komunikasi yang cepat, dan infrastruktur terkait lainnya.
 4. Bangunan Cerdas: Ini mengacu pada bangunan yang dilengkapi dengan teknologi cerdas untuk mengoptimalkan penggunaan energi, meningkatkan kenyamanan, dan meningkatkan produktivitas termasuk sistem manajemen energi bangunan, pencahayaan adaptif, sistem HVAC yang terhubung, dan lain-lain.
 5. Transportasi Cerdas: Ini melibatkan penggunaan teknologi cerdas dalam transportasi untuk meningkatkan mobilitas, keamanan, dan efisiensi termasuk penggunaan kendaraan otonom, sistem transportasi berbagi, monitoring lalu lintas cerdas, dan lain-lain.
 6. Sistem Kesehatan Cerdas: Ini mencakup penerapan teknologi cerdas dalam layanan kesehatan untuk memantau kesehatan, mendiagnosis penyakit, dan meningkatkan aksesibilitas layanan kesehatan dan termasuk penggunaan perangkat medis yang terhubung, sistem pemantauan kesehatan jarak jauh, dan platform manajemen data kesehatan.
 7. Industri Cerdas: Ini mengacu pada penerapan teknologi cerdas dalam industri untuk meningkatkan efisiensi, produktivitas, dan keamanan termasuk pabrik dengan sistem otomatis, sistem manufaktur adaptif, analisis prediktif untuk pemeliharaan mesin, dan lain-lain.

Dengan mengintegrasikan teknologi cerdas dalam berbagai aspek kehidupan sehari-hari, lingkungan cerdas dapat meningkatkan kualitas hidup, efisiensi, dan keberlanjutan secara

keseluruhan. Secara luas, lingkungan cerdas mencakup keterkaitan antara keseluruhan penerapan teknologi cerdas dalam kehidupan sehari-hari.



Gambar 12.2. Lingkungan Cerdas
(Sumber : (Ahmed *et al.*, 2016))

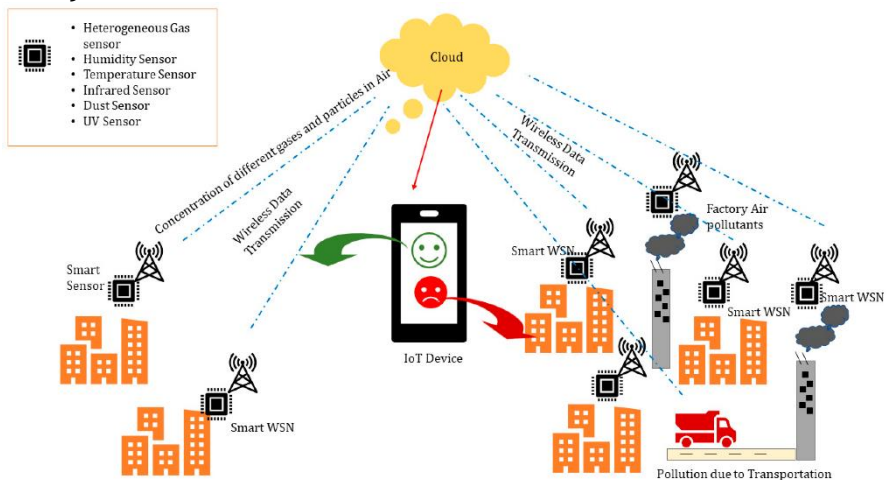
Penerapan teknologi ini memiliki potensi untuk memberikan dampak positif yang signifikan bagi perkembangan manusia dan keterhubungan dengan lingkungan sekitarnya. Dengan menggunakan teknologi IoT dalam lingkungan yang cerdas, kita dapat menghasilkan lingkungan yang lebih modern dan sejahtera. Hal ini tercapai melalui berbagai upaya, termasuk peningkatan efisiensi energi, pengelolaan sumber daya yang lebih efektif, penyediaan layanan yang lebih efisien dan terjangkau, serta peningkatan kesadaran akan lingkungan. Selain itu, adopsi lingkungan cerdas juga memungkinkan terciptanya interaksi yang lebih harmonis antara manusia dan lingkungan sekitar, termasuk dengan makhluk hidup lainnya dan alam secara keseluruhan. Dengan menggunakan sensor dan teknologi terhubung lainnya, kita dapat mengawasi kondisi lingkungan dengan lebih teliti, memahami

dampak aktivitas manusia, dan mengambil langkah-langkah yang tepat untuk melindungi dan merawat keberlanjutan alam. Pemanfaatan sensor dan teknologi IoT dalam interaksi manusia dengan lingkungan alam juga membuka peluang baru untuk pendekatan yang lebih proaktif terhadap pelestarian alam dan keberlanjutan. Misalnya, sensor yang terpasang di hutan dapat membantu dalam memonitor kebakaran hutan secara real-time, sehingga memungkinkan respon yang cepat dalam upaya pemadaman api dan perlindungan terhadap lingkungan serta kehidupan liar yang terpengaruh. Dengan demikian, penerapan lingkungan cerdas berbasis IoT tidak hanya memberikan manfaat bagi kemajuan teknologi dan kesejahteraan manusia, tetapi juga membantu menciptakan hubungan yang lebih harmonis antara manusia, makhluk hidup lainnya, dan alam sekitarnya. Hal ini merupakan langkah positif menuju masa depan yang lebih berkelanjutan dan seimbang.

12.2 Smart Environment Monitoring (SEM)

Smart Environment Monitoring (SEM) adalah sistem yang memanfaatkan teknologi sensor, jaringan nirkabel, dan analisis data untuk mengawasi dan mengelola keadaan lingkungan secara langsung. Tujuan utamanya adalah menghimpun informasi yang akurat tentang berbagai faktor lingkungan seperti kualitas udara, air, suhu, kelembaban, dan tingkat kebisingan. Sistem SEM biasanya terdiri dari beberapa bagian, termasuk sensor yang ditempatkan di lokasi strategis untuk mengukur faktor-faktor lingkungan, perangkat pengumpul data yang bertugas mengumpulkan dan menyimpan data dari sensor, jaringan komunikasi yang menghubungkan semua bagian, serta sistem analisis data yang mampu mengolah informasi yang didapat dan membuat laporan yang informatif. Dengan memadukan teknologi ini, SEM memungkinkan pengguna untuk mendapatkan pemahaman yang lebih baik tentang lingkungan sekitar mereka, memperoleh informasi secara real-time, dan merespons dengan cepat terhadap perubahan atau masalah yang mungkin timbul. Ini merupakan salah satu alat yang penting dalam mendukung usaha-usaha pemantauan

dan pengelolaan lingkungan yang berkelanjutan (Ullo and Sinha, 2020).



Gambar 12.3. Penerapan SEM
(Sumber : (Ullo and Sinha, 2020))

SEM pada lingkungan cerdas dalam konteks ini merujuk pada penggunaan teknologi untuk memantau dan mengelola aspek-aspek lingkungan yang berdampak langsung pada kehidupan sehari-hari manusia, seperti kualitas udara dan air. Ini melibatkan penerapan sensor dan solusi IoT untuk memantau parameter lingkungan yang krusial bagi kesehatan dan kenyamanan manusia.

Misalnya, dalam hal kualitas udara, sistem lingkungan cerdas dapat memantau tingkat polutan seperti partikulat, ozon, karbon monoksida, dan senyawa organik volatil. Sementara itu, untuk kualitas air, sistem tersebut dapat memantau parameter seperti kekeruhan, pH, TDS (*Total Dissolved Solids*), dan kandungan bahan kimia berbahaya.

Tujuan utamanya adalah untuk memberikan informasi yang akurat dan real-time kepada masyarakat tentang kondisi lingkungan sekitar mereka, sehingga mereka dapat mengambil tindakan yang sesuai untuk menjaga kesehatan dan kenyamanan mereka. Ini bisa termasuk memberikan peringatan dini tentang tingkat polusi udara yang tinggi atau memberi tahu tentang kualitas air yang tidak aman

untuk dikonsumsi. Dengan demikian, lingkungan cerdas dapat berkontribusi secara signifikan pada meningkatkan kualitas hidup dan kesejahteraan manusia di perkotaan.

12.3 Sensor Pendeteksi Kondisi Lingkungan

Kondisi lingkungan memainkan peran krusial dalam kehidupan sehari-hari manusia. Perbedaan antara lingkungan perkotaan dan pedesaan sangat mencolok. Di perkotaan, aktivitas padat, polusi udara, dan kebisingan seringkali menjadi bagian dari kehidupan sehari-hari. Lingkungan perkotaan juga cenderung memiliki infrastruktur yang lebih padat dan kompleks, dengan akses yang mudah terhadap berbagai layanan dan fasilitas.

Sementara itu, di pedesaan, lingkungan cenderung lebih tenang dan alami. Udara lebih segar, kepadatan penduduk lebih rendah, dan hubungan sosial biasanya lebih dekat. Aktivitas sehari-hari juga seringkali berkaitan dengan alam, seperti pertanian, peternakan, dan kegiatan outdoor lainnya. Meskipun mungkin kurangnya akses terhadap beberapa fasilitas modern, banyak orang menghargai kehidupan yang lebih sederhana dan dekat dengan alam di pedesaan.

Perbedaan ini mengilustrasikan betapa pentingnya lingkungan dalam menentukan kualitas hidup dan pengalaman manusia sehari-hari, serta menunjukkan perlunya pendekatan yang berbeda dalam mengelola dan merancang lingkungan perkotaan dan pedesaan.

Peran teknologi sangat besar dalam menjaga atau mengendalikan kondisi lingkungan perkotaan yang nyaman. Sensor-sensor ditempatkan di beberapa titik strategis di perkotaan untuk mendeteksi berbagai parameter lingkungan yang penting. Misalnya, sensor polusi udara digunakan untuk mengukur konsentrasi berbagai polutan udara seperti partikel halus (PM_{2.5}), karbon monoksida (CO), dan dioksida sulfur (SO₂) (Nugroho *et al.*, 2023). Sensor kondisi air dipasang di sungai-sungai untuk memantau tingkat kekeruhan, pH, oksigen terlarut, dan kehadiran zat-zat pencemar lainnya. Selain itu, sensor suhu dan kelembapan udara digunakan untuk memantau kondisi termal perkotaan.

Data yang dikumpulkan oleh sensor-sensor ini dikirim secara real-time ke pusat pemantauan lingkungan. Pihak berwenang dapat menggunakan informasi ini untuk mengambil tindakan yang cepat dan tepat guna memantau dan memperbaiki kualitas lingkungan di perkotaan. Misalnya, jika sensor menunjukkan peningkatan kadar polutan udara di suatu wilayah, pihak berwenang dapat segera mengirimkan peringatan kepada penduduk setempat atau mengatur langkah-langkah mitigasi seperti pembatasan lalu lintas atau pengurangan emisi industri.

Dengan adanya teknologi sensor ini, pemantauan lingkungan menjadi lebih efisien dan efektif. Hal ini membantu menjaga kualitas udara, air, dan lingkungan perkotaan secara keseluruhan, serta meningkatkan kenyamanan dan kesehatan masyarakat perkotaan.

12.4 Sensor Kualitas Udara

Pemantauan tingkat CO dan SO₂ di lingkungan perkotaan sangat penting untuk melindungi kesehatan manusia dan menjaga kualitas udara. Pemaparan terhadap CO dapat menyebabkan keracunan, gejala seperti sakit kepala, mual, muntah, dan bahkan kematian jika terjadi dalam kadar yang tinggi dan dalam waktu yang lama. SO₂ juga dapat menyebabkan iritasi pada saluran pernapasan, terutama pada orang-orang dengan masalah pernapasan seperti asma atau penyakit paru obstruktif kronis (PPOK). Selain itu, SO₂ dapat bereaksi dengan partikel lain dalam udara dan membentuk kabut asam, yang dapat merusak tanaman, bangunan, dan lingkungan perairan.

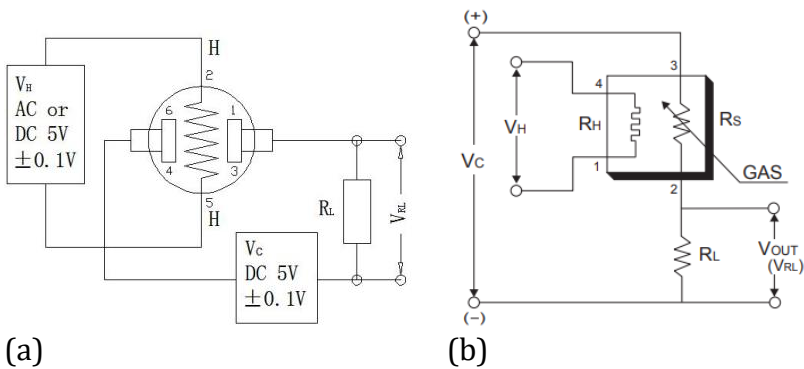
Terdapat berbagai sensor yang dapat digunakan untuk mendeteksi kualitas udara, baik untuk kelas proyek kecil hingga skala industri antara lain yang dibuat oleh Perusahaan Zhengzhou Winsen Electronics Technology Co., Ltd. Untuk sensor seri MQ-x dan Figaro Engineering Inc. untuk sensor dengan seri TGS-x:

Tabel 12.1. Sensor Gas dan Kualitas Udara

Tipe sensor	Target pendeteksian	Jangkauan pendeteksian	Bentuk fisik
MQ-2	Methane, Butane, LPG, smoke	300-10000 ppm(Flammable gas)	
MQ-4	Methane, CNG Gas	300~10000ppm	
MQ-5	Natural gas, LPG	300~10000ppm	
MQ-7B	Carbon Monoxide	10~500ppm CO	
MQ-8	Hydrogen Gas	100~1000 ppm(H2)	
MQ-9B	Carbon Monoxide, flammable gasses	10~500ppm CO, 300~10000 ppm CH4	
MQ131	High Concentration - Ozone	10~1000 ppm Ozone	
MQ131	Low Concentration - Ozone	10~1000 ppb Ozone	
MQ135	Air Quality (CO, Ammonia, Benzene, Alcohol, smoke)	10~1000 ppm (ammonia gas, toluene, Hydrogen, smoke)	
MQ136	Hydrogen Sulfide gas	1~200 ppm H2S	
MQ137	Ammonia	5~500 ppm NH3	
MQ138	Benzene, Toluene, Alcohol, Acetone, Propane, Formaldehyde gas, Hydrogen	5~500 ppm VOC	
MQ303B	Alcohol, C2H5OH	20~ 500ppm alcohol	

Type sensor	Target pendeteksian	Jangkauan pendeteksian	Bentuk fisik
TGS 2620	Alkohol	200~10000 ppm	
TGS2600	Air Contaminants	1~100 ppm	
TGS 2610	LPG propane butane	200~4000 ppm	
TGS2611	Methane Natural Gas	200~10000 ppm	

(Sumber : <https://www.winsen-sensor.com/>,
<https://www.figaro.co.jp/>)



Gambar 12.3. Rangkaian Sensor (a) tipe MQ-x dan (b) TGS-x
(Sumber : datasheets MQ-2 dan datasheets TGS2600)

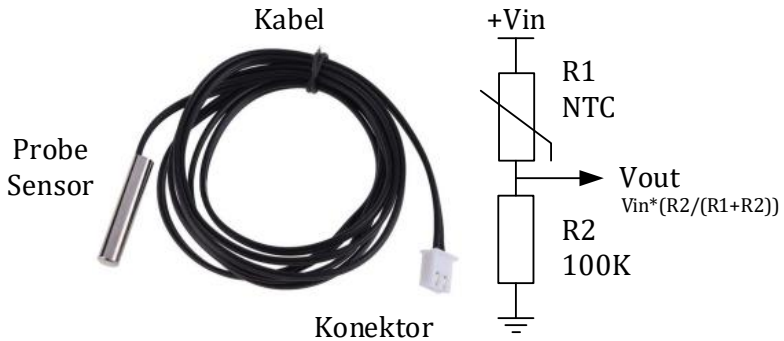
Sensor tersebut membutuhkan resistor tambahan untuk dapat dapat terhubung dengan Arduino untuk pemantauan atau perangkat lain semisal komparator operasional amplifier (OP-Amp) untuk rangkaian penginderaan dan proteksi.

12.5 Sensor Kualitas Air

Berdasarkan SNI 01-3553-2006 tentang standar air minum, ada tiga aspek utama yang diatur: fisik, kimia, dan bakteriologis. Standar fisik mencakup berbagai parameter seperti warna, aroma, rasa, suhu, dan tingkat kekeruhan. Kekeruhan air dapat disebabkan oleh beragam bahan, baik organik maupun anorganik, seperti lumpur dan limbah. Standar kimia mengatur kandungan senyawa dan logam berbahaya dalam air, seperti merkuri, timbal, perak, tembaga, dan seng, serta residu pestisida yang dapat memengaruhi karakteristik fisik dan kimia air. Sementara itu, standar bakteriologis, sesuai dengan peraturan Menteri Kesehatan Republik Indonesia Nomor 907/Menkes/SK/VII/2002, menegaskan bahwa air minum tidak boleh mengandung bakteri patogen yang dapat menyebabkan penyakit saluran pencernaan. Secara umum, penilaian kualitas air bersih melibatkan beberapa parameter penting, seperti Total Dissolved Solids (TDS), tingkat kekeruhan, suhu, warna, kandungan besi (Fe^{2+}), konsentrasi fluorida (F), kadar klorida, kadar mangan (Mn), kadar nitrit (NO_2^-), tingkat keasaman (pH), kandungan sulfat (SO_4^{2-}), dan jumlah total koliforma/E. coli. Parameter-parameter ini memberikan gambaran holistik tentang kondisi dan kebersihan air, serta dapat digunakan sebagai acuan untuk menilai tingkat kesesuaian air tersebut untuk konsumsi manusia atau penggunaan lainnya (Db, Satyanto and Saptomo, 2019).

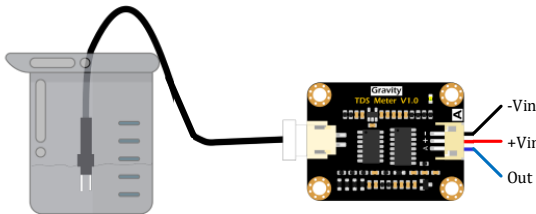
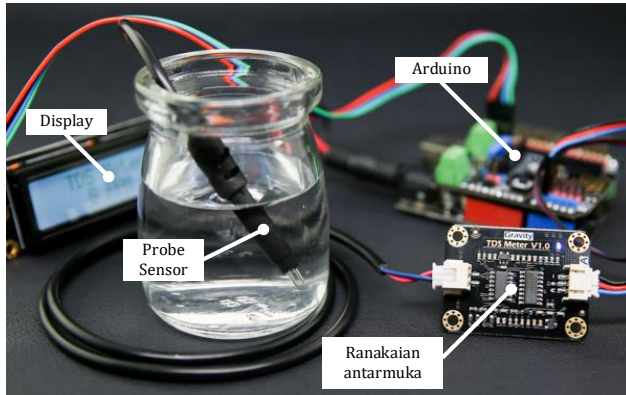
Sensor yang tersedia digunakan untuk mengukur kualitas fisik dari air antara lain:

1. Sensor Thermistor NTC 3950 Waterproof Temperature Probe digunakan untuk mengukur suhu dalam air. Sensor ini memiliki kemampuan untuk mengukur suhu dalam rentang -20 hingga 105 derajat Celsius. Sensor ini dapat membutuhkan tambahan resistor pembagi tegangan dengan nilai 100 Kohm untuk dapat dihubungkan dengan pin analog pada Arduino atau dapat juga dihubungkan dengan penguat operasional untuk meningkatkan sensitivitas pengukuran.



Gambar 12.4. Sensor Thermistor NTC 3950
(Sumber : <https://www.tokopedia.com/>)

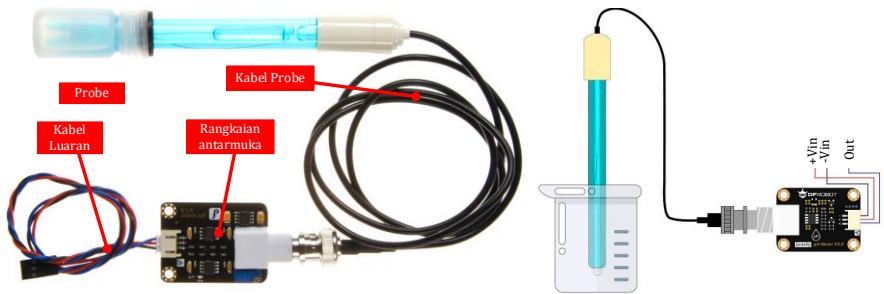
2. TDS (*Total Dissolved Solids*) mengindikasikan jumlah padatan yang terlarut dalam satu liter air. Secara umum, semakin tinggi nilai TDS, semakin banyak padatan terlarut yang ada dalam air, menunjukkan tingkat kebersihan air yang rendah. Oleh karena itu, nilai TDS dapat digunakan sebagai indikator untuk menilai kualitas air. DFrobot telah membuat sensor TDS yang membutuhkan tegangan masukan antara 3,3 hingga 5,5V, dan memberikan keluaran tegangan analog antara 0 hingga 2,3V, sehingga kompatibel dengan berbagai sistem atau papan kontrol yang bekerja pada tegangan 5V atau 3,3V, seperti Arduino, ESP32, Raspberry Pi, micro:bit, dan LattePanda. Sinyal eksitasi probe berbentuk AC, yang membantu mencegah polarisasi probe dan meningkatkan umur pakai serta stabilitas sinyal keluaran. Probe TDS juga tahan air, sehingga dapat digunakan untuk pengukuran dalam jangka waktu yang lama bahkan saat terendam dalam air (dfrobot.com, 2024).



Gambar 12.5. Sensor Thermistor NTC 3950
(Sumber : <https://wiki.dfrobot.com/>)

PH adalah ukuran yang menunjukkan tingkat keasaman atau alkalinitas suatu larutan, juga dikenal sebagai indeks konsentrasi ion hidrogen. PH mencerminkan aktivitas ion hidrogen dalam larutan dan memiliki beragam aplikasi dalam bidang seperti kedokteran, kimia, dan pertanian. Rentang pH biasanya antara 0 hingga 14, dengan nilai 7 menunjukkan larutan netral dalam kondisi standar termodinamika. Larutan dengan $\text{pH} < 7$ dianggap asam, sementara $\text{pH} > 7$ menunjukkan sifat basa.

Salah satu produk sensor pH yang tersedia adalah dari DFRobot, yang memiliki tingkat ketelitian tinggi. Catu daya internal modul sensor ini memiliki rentang 3.3 hingga 5.5V, sehingga kompatibel dengan berbagai mikrokontroler yang beroperasi pada 5V dan 3.3V. Sinyal keluaran dari sensor ini telah disaring oleh perangkat keras, menghasilkan noise yang rendah. Program library yang disediakan juga mendukung metode kalibrasi dua titik, dan secara otomatis mengenali dua larutan buffer standar ($\text{pH} 4.0$ dan 7.0) (dfrobot.com, 2024).



Gambar 12.6. Sensor PH

(Sumber : <https://www.dfrobot.com/product-1782.html>)

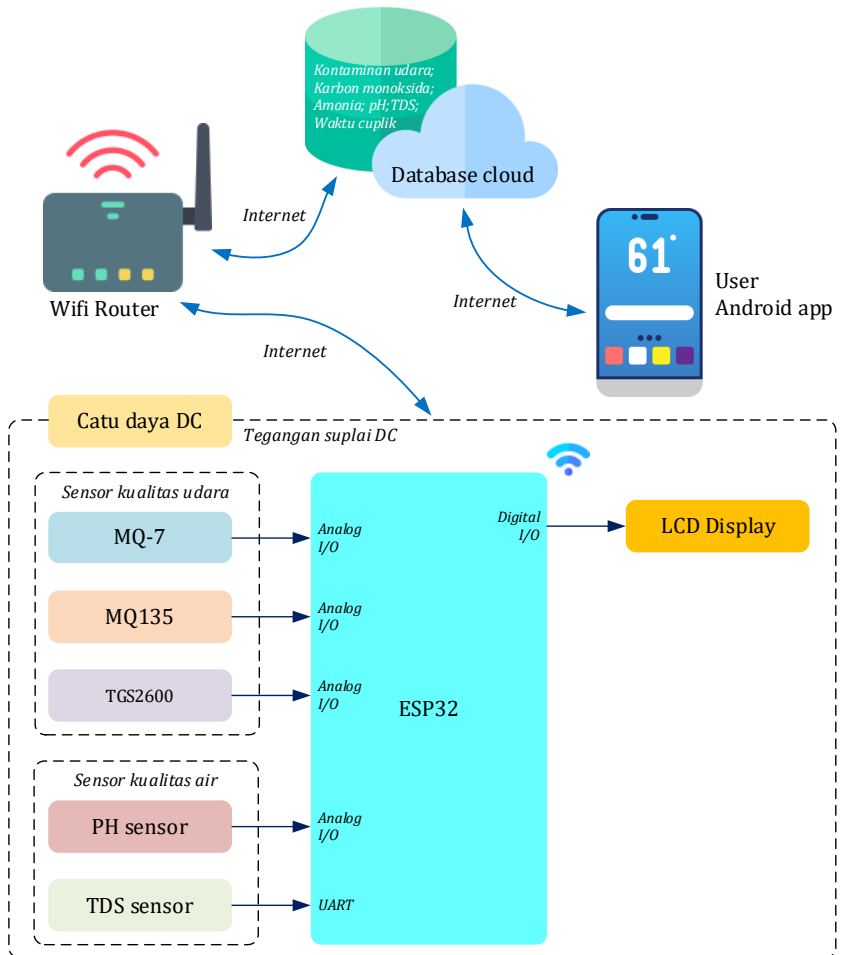
12.6 Pemantauan Kualitas Udara dan Air Berbasis ESP32

Teknologi sensor dan IoT memiliki potensi besar untuk diterapkan dalam pendeteksian kondisi lingkungan seperti kualitas udara dan air. Sistem ini dapat diterapkan dalam konteks *smart-city*, *smart-building*, atau *smart-industri* untuk mengawasi kondisi udara, kebersihan air, dan limbah. Keluaran dari perangkat ini dapat berupa peringatan atau alarm yang memberitahu pengguna tentang kondisi yang tidak normal, serta dapat digunakan sebagai referensi untuk mengambil tindakan yang tepat. Dengan demikian, teknologi ini tidak hanya membantu dalam menjaga kualitas lingkungan, tetapi juga meningkatkan responsivitas terhadap perubahan kondisi lingkungan yang mungkin berdampak pada kesehatan dan keamanan manusia serta keberlanjutan lingkungan.

Sistem pemantauan kualitas air dan udara berbasis IoT sederhana memiliki komponen-komponen utama sebagai berikut:

1. Esp32: Microcontroller yang berfungsi sebagai otak sistem, menghubungkan nilai-nilai sensor dengan internet, dan mengatur fungsi-fungsi sistem secara keseluruhan.
2. Catu daya: Memasok listrik untuk sistem agar dapat beroperasi secara optimal. Terdapat dua level tegangan yang digunakan yaitu 3.3 volt untuk suplai ESP32 dan 5 volt untuk suplai sensor.
3. Sensor MQ-7: Digunakan untuk mendeteksi konsentrasi gas karbon monoksida (CO) dalam udara.

4. Sensor MQ-135: Sensor untuk mendeteksi kualitas udara secara umum, termasuk konsentrasi beberapa gas beracun seperti amonia, benzene, dan karbon dioksida (CO₂).
5. Sensor TGS2600: Sensor untuk mendeteksi konsentrasi gas berbahaya seperti amonia, hidrogen, dan gas-gas lainnya.
6. Sensor pH: Digunakan untuk mengukur tingkat keasaman atau alkalinitas larutan air.
7. Sensor TDS: Sensor untuk mengukur total padatan terlarut dalam air, yang mencerminkan tingkat kebersihan air.
8. LCD display: Digunakan untuk menampilkan informasi yang diperoleh dari sensor-sensordan digunakan dalam pemantauan jarak dekat atau langsung. Nilai yang dapat ditampilkan antara lain pH, TDS, dan konsentrasi gas.
9. Wifi router: Menyediakan koneksi internet yang diperlukan untuk mengirimkan data dari sensor ke database cloud dan perangkat lainnya.
10. Database cloud: Tempat penyimpanan data secara online, yang memungkinkan pengguna untuk mengakses informasi mengenai kualitas air dan udara dari mana saja.
11. HP android: Digunakan sebagai perangkat untuk mengakses dan memantau data kualitas air dan udara yang tersimpan di database cloud, serta menerima pemberitahuan atau alarm jika terdeteksi adanya kondisi yang tidak normal.



Gambar 12.7. Diagram Sistem Pemantauan Lingkungan Berbasis IoT

(Sumber icon & simbol: <https://www.flaticon.com/>)

Dengan adanya sistem ini, pengguna dapat memantau secara real-time kualitas air dan udara di suatu lokasi tertentu, serta melakukan intervensi atau tindakan yang diperlukan untuk menjaga lingkungan tetap bersih dan sehat.

DAFTAR PUSTAKA

- Ahmed, E. *et al.* (2016) 'Internet-of-things-based smart environments: State of the art, taxonomy, and open research challenges', *IEEE Wireless Communications*, 23(5), pp. 10–16. Available at: <https://doi.org/10.1109/MWC.2016.7721736>.
- dfrobot.com (2024) *Analog TDS Sensor Meter for Arduino / ESP32 / Raspberry Pi - DFRobot Wiki*, wiki.dfrobot.com. Available at: https://wiki.dfrobot.com/Gravity_Analog_TDS_Sensor_Meter_For_Arduino_SKU_SEN0244 (Accessed: 5 May 2024).
- caburntelecom.com (2024) *What is IoT Environmental Monitoring?*, <https://caburntelecom.com/>. Available at: <https://caburntelecom.com/iot-environmental-monitoring/> (Accessed: 5 May 2024).
- Db, M.H., Satyanto, D. and Saptomo, K. (2019) *Analisis Kualitas Air pada Jalur Distribusi Air Bersih di Gedung Baru Fakultas Ekonomi dan Manajemen Institut Pertanian Bogor (Analysis of Water Quality of Water Distribution Channels in New Building of Faculty of Economics and Management Bogor Agricultural University (IPB))*.
- Ikrisi, G. and Mazri, T. (2021) 'IoT-Based Smart Environments: State Of The Art, Security Threats And Solutions', in *International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences - ISPRS Archives*. International Society for Photogrammetry and Remote Sensing, pp. 279–286. Available at: <https://doi.org/10.5194/isprs-Archives-XLVI-4-W5-2021-279-2021>.
- Nugroho, Y.C. *et al.* (2023) 'Rancang Bangun Sistem Pemantauan Kualitas Udara Berbasis Arduino Untuk Mendeteksi Polusi Udara Di Perkotaan', *Jurnal TIKomSiN*, 11(2), pp. 45–52. Available at: <https://doi.org/https://doi.org/10.30646/tikomsin.v11i2.795>.
- dfrobot.com (2024) *PH_meter_SKU_SEN0161_DFRobot*, wiki.dfrobot.com. Available at: https://wiki.dfrobot.com/PH_meter_SKU_SEN0161_ (Accessed: 5 May 2024).

Ullo, S.L. and Sinha, G.R. (2020) 'Advances in smart environment monitoring systems using iot and sensors', *Sensors (Switzerland)*. MDPI AG. Available at: <https://doi.org/10.3390/s20113113>.

BIODATA PENULIS



Dr. Purnawarman Musa, S.Kom., M.T., M.I.Kom

Dosen Program Studi Teknik Elektro
Fakultas Teknologi Industri

Penulis lahir di Gorontalo pada tahun 1975 sebagai dosen tetap di Universitas Gunadarma, menyelesaikan pendidikan pada program studi *Electronic Image and Informatic* dengan gelar Doktor (Dr.) pada bidang Teknologi Infomasi dari Burgundy of University di kota Dijon, France pada tahun 2013. Penulis memperoleh gelar *Master of Engineering* (M.T.) tahun 2006 di Universitas Gunadarma Jakarta - Indonesia, gelar *Master of Communication* (M.I.Kom) tahun 2021 di Universitas Gunadarma, Jakarta - Indonesia dan tahun 1999 menyelesaikan pendidikan S1 jurusan *Computer Engineering* (S.Kom) di Universitas Gunadarma, Jakarta - Indonesia. Penulis menekuni bidang Robotika, IoT, Computer Vision, Kecerdasan Buatan, Remote Sensing dan Sistem Tertanam. Beberapa keanggota penulis, diantaranya Ikatan Ahli Informatika Indonesia (IAII) dan Asosiasi Perguruan Tinggi Informatika dan Komputer (APTIKOM).

BIODATA PENULIS



Amin Ama Duwila, ST.,M.Sc.

ASN Pemda Kabupaten Halmahera Selatan

Penulis lahir di Labuha Kecamatan Bacan tanggal 28 Mei 1972. Penulis adalah ASN Pemda Kabupaten Halmahera Selatan Provinsi Maluku Utara. Menyelesaikan pendidikan S1 pada Fakultas Teknik Universitas Pattimura - Ambon dan melanjutkan S2 pada Magister Sistem dan Teknik Transportasi (MSTT) Universitas Gadjah Mada (UGM) - Yogyakarta. Penulis menekuni bidang menulis pada tema transportasi, kebencanaan dan teknologi informasi berdasarkan kualifikasi pendidikan dan pengalaman selama bertugas pada perusahaan BUMN dan sebagai ASN pada Pemerintah Daerah Kabupaten Halmahera Selatan yang pernah ditempatkan sebagai Kasubag. Perencanaan dan Evaluasi Program, Kepala Seksi Telekomunikasi, Kepala Bidang Perhubungan Udara dan Telekomunikasi dan saat ini sebagai Sekretaris Dinas Perhubungan Kabupaten Halmahera Selatan.

BIODATA PENULIS



Muhammad Irwan Syahib, S.T., M.Kom.

Dosen Program Studi Sistem dan Teknologi Informasi
Fakultas Teknik

Penulis saat ini beraktifitas sebagai tenaga pengajar di Program Studi Sistem dan Teknologi Informasi Fakultas Teknik Universitas Muhammadiyah Kendari. Menyelesaikan pendidikan S1 di Jurusan Teknik Informatika Universitas Halu Oleo dan melanjutkan S2 di Jurusan Teknik Informatika Universitas Ahmad Dahlan Yogyakarta. Penulis juga menekuni bidang Jaringan komputer dan digital forensik dan sedang berfokus pada penelitian bidang forensik kejahatan mobile, system informasi dan jaringan komputer.

BIODATA PENULIS



Alex Copernikus Andaria, S.T., M.Pd.

Dosen Program Studi Sistem Komputer

Fakultas Ilmu Pengetahuan, Teknologi dan Keguruan Universitas
Trinita

Penulis lahir di Manado 18 April 1984. Penulis adalah dosen tetap pada Program Studi Sistem Komputer Fakultas Ilmu Pengetahuan, Teknologi dan Keguruan, Universitas Trinita. Menyelesaikan pendidikan S1 pada Jurusan Teknik Elektro dan Informatika Universitas Sam Ratulangi dan melanjutkan S2 pada Jurusan Pendidikan Teknologi dan Kejuruan Universitas Negeri Manado. Selain aktif dalam kegiatan penelitian dan pengembangan di bidang sistem komputer dan teknologi pembelajaran, dengan semangat dan dedikasi yang tinggi, penulis berusaha untuk membagikan ilmu dan pengalamannya kepada para mahasiswa lewat buku ini, khususnya untuk mata kuliah yang diampu penulis yaitu Sistem Digital, Sensor dan Transduser, serat Periferal dan Antarmuka.

BIODATA PENULIS



Yendi Putra, S. Kom., M. Kom, MTA

Dosen Program Studi Manajemen Informatika
Fakultas Eknomi Universitas Mahaputra Muhammad Yamin

Penulis lahir di Salimpuang tanggal 03 Januari 1988. Penulis adalah dosen tetap pada Program Studi Manajemen Informatika Fakultas Eknomi 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. 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



Kusnaeni, M.Si.

Dosen Program Studi Sistem Energi
Jurusan Teknologi Produksi dan Industri

Penulis lahir di Makassar tanggal 16 Januari 1995. Penulis adalah dosen tetap pada Program Studi Sistem Energi Jurusan Sains, Institut Teknologi Bacharuddin Jusuf Habibie. Menyelesaikan pendidikan S1 pada Jurusan Matematika Universitas Hasanuddin dan melanjutkan S2 pada Jurusan Statistika dan Sains Data Institut Pertanian Bogor. Penulis menekuni penelitian-penelitian pada bidang Sains Data

BIODATA PENULIS

Ir. Hamdan Gani, S.Kom., MT., Ph.D

Dosen Program Studi Otomasi Sistem Permesinan
Politeknik ATI Makassar

Penulis lahir di Ujung Pandang tanggal 23 November 1988. Penulis adalah dosen tetap pada Program Studi Program Studi Otomasi Sistem Permesinan Politeknik ATI Makassar. Menyelesaikan pendidikan S1 pada Jurusan Teknik Informatika UIN Alauddin Makassar, S2 pada Jurusan Teknik Elektro Universitas Hasanuddin dan Melanjutkan S3 di Kyushu University Jepang dan terakhir melanjutkan pendidikan profesi Insinyur pada Universitas Muslim Indonesia (UMI).

BIODATA PENULIS



Muhammad Fadli Azis, S.T., M.Sc.

Dosen Program Studi Otomasi Sistem Permesinan
Politeknik ATI Makassar Kementerian Perindustrian RI

Penulis lahir di Lampa tanggal 02 Juni 1992. Penulis adalah dosen tetap pada Program Studi Otomasi Sistem Permesinan Politeknik ATI Makassar Kementerian Perindustrian RI. Penulis menyelesaikan pendidikan S1 pada Jurusan Teknik Elektro Sistem Tenaga di Institut Teknologi Sepuluh November (ITS) Surabaya pada tahun 2015. Selanjutnya penulis menyelesaikan pendidikan S2 pada Jurusan Electrical Power System di University of Manchester (UoM) United Kingdom pada tahun 2017.

BIODATA PENULIS



Asma Ainuddin, S.Kom., M.T.

Dosen Program Studi Teknik Listrik dan Instalasi
Akademi Komunitas Industri manufaktur Bantaeng

Penulis lahir di Majene Sulawesi Barat tanggal 11 Maret 1991. Penulis adalah dosen tetap pada Program Studi Teknik Listrik dan Instalasi, Akademi Komunitas Industri Manufaktur Bantaeng. Menyelesaikan pendidikan S1 pada Jurusan Sistem Komputer STMIK Handayani Makassar dan melanjutkan S2 pada Jurusan Teknik Elektro Universitas Hasanuddin. Penulis menekuni bidang Komputer dan Kendali.

BIODATA PENULIS



Julianti Habibuddin, S.T.,M.T

Dosen Program Studi Otomasi Sistem Permesinan
Politeknik ATI Makassar

Penulis lahir di Ujung Pandang tanggal 23 Juli 1989. Penulis adalah dosen tetap pada Program Studi Otomasi Sistem permesian Politeknik ATI Makassar. Menyelesaikan pendidikan S1 pada Jurusan Teknik Elektro Universitas Hasanuddin dan melanjutkan S2 pada Jurusan Teknik Elektro Universitas Hasanuddin.

BIODATA PENULIS



Muhammad Sainal Abidin, S.Si., M.Si.

Dosen Program Studi D-III teknologi elektro-medis
Fakultas Sains Dan Teknologi
Universitas Mandala Waluya

Penulis lahir di Kendari tanggal 16 Desember 1987. Penulis adalah dosen program studi D-III teknologi Elektro-Medis Fakultas Sains Dan Teknologi Universitas Mandala Waluya. Menyelesaikan pendidikan S1 pada Fisika MIIPA Universitas Haluoleo dan melanjutkan S2 pada Jurusan Fisika Institut Teknologi Bandung dengan Kelompok Keahlian Fisika Instrumentasi. Penulis menekuni bidang instrumentasi dengan penelitian berfokus pada pengembangan alat kesehatan.

BIODATA PENULIS



Tino Suhaebri, S.ST., M.T.

Dosen Program Studi Teknik Listrik dan Instalasi
Akademi Komunitas Industri Manufaktur Bantaeng

Penulis lahir di Ujung Pandang, Sulawesi Selatan, pada tanggal 18 Juni 1988. Saat ini, penulis menjabat sebagai dosen tetap di Program Studi Teknik Listrik dan Instalasi di Akademi Komunitas Industri Manufaktur Bantaeng. Sebelumnya, penulis menempuh pendidikan di bidang teknik elektronika di STM Pembangunan Makassar, kemudian melanjutkan studi D3 Teknik Elektronika dan D4 Teknik Listrik di Politeknik Negeri Ujung Pandang. Selanjutnya, penulis meraih gelar S2 di Jurusan Teknik Elektro dari Universitas Hasanuddin. Penulis memiliki minat dan pengalaman yang luas dalam bidang Elektronika, Robotik, dan Kendali.