

TRANSFORMASI DIGITAL: MEMAHAMI INTERNET OF THINGS



Muhammad Rizal, Arief Yanto Rukmana, Irmawati,
Angga Aditya Permana, Melissa Indah Fianty, Heru Saputra,
Fahmy Rinanda Saputri, Suwito Pomalingo, Rudi Sutomo,
Risanto Darmawan, Niko Akbar, Iwan Adhicandra

TRANSFORMASI DIGITAL: MEMAHAMI INTERNET OF THINGS

**Muhammad Rizal
Arief Yanto Rukmana
Irmawati
Angga Aditya Permana
Melissa Indah Fianty
Heru Saputra
Fahmy Rinanda Saputri
Suwito Pomalingo
Rudi Sutomo
Risanto Darmawan
Niko Akbar
Iwan Adhicandra**



GET PRESS INDONESIA

TRANSFORMASI DIGITAL: MEMAHAMI INTERNET OF THINGS

Penulis :

Muhammad Rizal
Arief Yanto Rukmana
Irmawati
Angga Aditya Permana
Melissa Indah Fianty
Heru Saputra
Fahmy Rinanda Saputri
Suwito Pomalingo
Rudi Sutomo
Risanto Darmawan
Niko Akbar
Iwan Adhicandra

ISBN : 978-623-198-666-5

Editor : Diana Purnama Sari., S.E M.E

Penyunting : Tri Putri Wahyuni, S.Pd

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, 6 September 2023

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 Transformasi Digital: Memahami Internet Of Things ini.

Buku ini membahas Pengantar Transformasi Digital, Konsep Dasar Internet of Things, Infrastruktur Internet of Things, Manfaat Internet of Things dalam Keberlanjutan, Internet of Things dalam Industri 4.0, Peran Internet of Things dalam Bisnis Digital, Internet of Things dalam Kesehatan, Keamanan dan Privasi dalam Internet of Things, Internet of Things dan Transportasi Masa Depan, Internet of Things dalam Rumah Pintar, Analitik Data dan Kecerdasan Buatan dalam Internet of Things, Tantangan dan Peluang Masa Depan dalam Internet of Things.

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, 6 September 2023

Penulis

DAFTAR ISI

KATA PENGANTAR	i
DAFTAR ISI	ii
DAFTAR GAMBAR	viii
DAFTAR TABEL	xi
BAB 1 PENGANTAR TRANSFORMASI DIGITAL.....	1
1.1 Definisi Transformasi Digital.....	1
1.2 Evolusi Transformasi Digital.....	2
1.3 Manfaat Transformasi Digital.....	4
1.4 Tantangan Transformasi Digital	5
DAFTAR PUSTAKA.....	7
BAB 2 KONSEP DASAR INTERNET OF THINGS	9
2.1 Pendahuluan	9
2.2 Memahami Dasar-Dasar IoT	11
2.3 Arsitektur IoT	14
2.4 Protokol Komunikasi IoT.....	16
2.5 Analisis Data IoT	19
2.6 Keamanan dan Privasi IoT.....	21
2.7 Aplikasi IoT dalam Transformasi Digital.....	23
2.8 Tren dan Tantangan Masa Depan IoT.....	26
DAFTAR PUSTAKA.....	30
BAB 3 INFRASTRUKTUR INTERNET OF THINGS.....	37
3.1 Pengenalan Infrastruktur Internet of Things	37
3.2 Komponen Infrastruktur IoT.....	38
3.2.1 Jaringan dan Protokol Komunikasi	40
3.2.2 Cloud Computing dan Edge Computing.....	41
3.3 Keamanan dalam Infrastruktur IoT.....	42
3.3.1 Tantangan Keamanan dan Privasi	44
3.4 Pengelolaan Perangkat IoT	46
3.5 Analisis Data IoT	48
3.5.1 Analisis Data dalam Infrastruktur IoT	49
3.6 Integrasi dan Interoperabilitas	50
3.6.1 Integrasi Infrastruktur IoT	52

3.7 Skalabilitas dan Fleksibilitas.....	54
3.8 Arsitektur Referensi IoT	56
3.8.1 Gambaran Model Arsitektur Referensi	57
3.9 Studi Kasus.....	58
3.9.1 Implementasi Infrastruktur IoT	60
DAFTAR PUSTAKA	62
BAB 4 MANFAAT INTERNET OF THINGS	
DALAM KEBERLANJUTAN.....	65
4.1 Pendahuluan.....	65
4.2 Peran IoT dalam Memonitoring Lingkungan.....	69
4.3 Peran IoT dalam Pengelolaan Sumber Daya	71
4.4 Peran IoT dalam Pertanian Berkelanjutan	74
4.5 Peran IoT dalam Pengelolaan Limbah	76
4.6 Peran IoT pada Mobilitas Cerdas	79
4.7 Peran IoT dalam Konversi Energi.....	82
4.8 Peran IoT dalam Pencegahan Bencana Alam.....	85
4.9 Peran IoT pada Pendidikan dan Kesadaran Lingkungan.....	88
DAFTAR PUSTAKA	91
BAB 5 INTERNET OF THINGS DALAM INDUSTRI 4.0	93
5.1 Pendahuluan.....	93
5.2 Industri 4.0.....	95
5.2.1 Revolusi industri: Phases of development	97
5.2.2 Evolusi Industri 4.0.....	100
5.2.3 Dampak lingkungan dari revolusi industri	102
5.2.4 Industrial Internet	102
5.2.5 Aplikasi di Industri 4.0	105
5.3 IIoT	106
5.3.1 Prerequisites pada IIoT	109
5.3.2 Dasar dari CPS.....	111
5.3.3 CPS dan IIoT	113
5.3.4 Aplikasi pada IIoT	114
5.4 Kesimpulan.....	116
DAFTAR PUSTAKA	118

BAB 6 PERAN INTERNET OF THINGS DALAM

BISNIS DIGITAL.....121

6.1 Pendahuluan121

6.1.1 Pengenalan Internet of Things (IoT)121

6.1.2 Pengenalan Bisnis Digital122

6.2 Peran IoT dalam Bisnis Digital.....123

6.2.1 Meningkatkan Efisiensi Operasional.....123

6.2.2 Meningkatkan Pengalaman Pelanggan124

6.2.3 Inovasi Produk dan Layanan.....124

6.2.4 Peningkatan Keamanan dan Keandalan.....126

6.3 Implementasi IoT dalam Berbagai Sektor Bisnis.....127

6.3.1 IoT dalam Retail127

6.3.2 IoT dalam Industri Manufaktur128

6.3.3 IoT dalam Transportasi dan Logistik.....130

6.3.4 IoT dalam Layanan Kesehatan.....131

6.3.5 IoT dalam Pertanian dan Pangan.....133

6.4 Tantangan dan Peluang dalam Mengadopsi IoT dalam Bisnis Digital134

6.6 Kesimpulan135

DAFTAR PUSTAKA.....136

BAB 7 INTERNET OF THINGS DALAM KESEHATAN137

7.1 Pendahuluan137

7.2 Internet of Things dalam Kesehatan139

7.3 Tantangan dan Solusi Penggunaan Internet of Things dalam Kesehatan dan Medis.....142

7.4 Permintaan dan Tantangan Keamanan untuk Beberapa Aplikasi IoT144

7.5 Contoh Metodologi dalam IoT di bidang Kesehatan147

7.6 Metodologi dalam IoT di bidang Kesehatan153

7.6.1 Diagnosis Jantung berbasis Arduino Kit dan IoT ...155

7.6.2 Diagnosis Otak berbasis Sinyal Data Klinis Real Time159

DAFTAR PUSTAKA.....164

BAB 8 KEAMANAN DAN PRIVASI DALAM

INTERNET OF THINGS	167
8.1 Pendahuluan.....	167
8.1.1 Pentingnya Keamanan dan Privasi dalam IoT	168
8.1.2 Konsep Keamanan Dan Privasi Dalam IoT.....	169
8.2 Ancaman Keamanan dan Privasi dalam IoT	170
8.2.1 Ancaman Keamanan dalam IoT	170
8.2.2 Ancaman Privasi dalam IoT.....	174
8.2.3 Kasus Nyata: Ancaman dan Implikasi dalam Dunia Nyata	176
8.3 Prinsip-prinsip Keamanan dan Privasi dalam IoT	177
8.3.1 Rancangan Keamanan (Security by Design).....	178
8.3.2 Prinsip Minimalisasi Data (<i>Data Minimization</i>).....	179
8.3.3 Prinsip Transparansi (Transparency).....	181
8.4 Strategi dan Teknologi untuk Mengamankan IoT	182
8.4.1 Proteksi Jaringan dan Sistem.....	182
8.4.2 Manajemen Identitas dan Akses	183
8.4.3 Teknologi Kriptografi.....	185
8.5 Regulasi dan Standar Keamanan dan Privasi IoT	186
8.5.1 Overview Regulasi Yang Ada	186
8.5.2 Standar Keamanan IoT.....	187
8.5.3 Dampak dan Tantangan Implementasi Regulasi Dan Standar	190
8.6 Tantangan dan Solusi Masa Depan untuk Keamanan dan Privasi IoT	191
8.6.1 Tantangan Dalam Implementasi Keamanan Dan Privasi IoT	191
8.6.2 Solusi Yang Dikembangkan Untuk Keamanan Dan Privasi IoT.....	192
8.6.3 Prediksi Tren Masa Depan Untuk Keamanan Dan Privasi IoT	193
8.7 Kesimpulan.....	195
DAFTAR PUSTAKA.....	197
BAB 9 INTERNET OF THINGS DAN TRANSPORTASI MASA DEPAN	201

9.1 Introduction.....	201
9.2 Benefits of the IoT in Transportation	205
9.2.1 Meningkatkan Efisiensi.....	206
9.2.2 Meningkatkan Keamanan	206
9.2.3 Mengurangi Emisi	207
9.2.4 Meningkatkan Pengalaman Pengguna	207
9.2.5 Meningkatkan Manajemen Logistik	207
9.3 Self-driving Cars	208
9.4 Smart Charging Station	209
9.5 Smart Parking.....	210
9.6 IoT System for Car Safety.....	211
9.7 Smart Public Transport.....	214
9.8 Vehicle Tracking Systems.....	217
9.9 Smart Traffic Management.....	223
DAFTAR PUSTAKA.....	228
BAB 10 INTERNET OF THINGS DALAM	
RUMAH PINTAR	231
10.1 Pendahuluan.....	231
10.2 Ekosistem IoT Smart Home.....	231
10.3 Perangkat Pintar	234
10.4 Otomatisasi Rumah.....	237
10.5 Monitoring dan keamanan Rumah	239
10.6 Manajemen Energi	241
10.7 Analitik dan Pengumpulan data.....	243
10.8 Penutup	246
DAFTAR PUSTAKA.....	247
BAB 11 ANALITIK DATA DAN KECERDASAN	
BUATAN DALAM INTERNET OF THINGS	251
11.1 Analitik Data.....	251
11.2 Kecerdasan Buatan (<i>Artificial Intelligence /AI</i>)	251
11.3 Hubungan analitik data dan Kecerdasan Buatan pada IOT.....	252
DAFTAR PUSTAKA.....	256
BAB 12 TANTANGAN DAN PELUANG MASA DEPAN	

DALAM INTERNET OF THINGS	259
12.1 Pendahuluan.....	259
12.1.1 Pengenalan tentang <i>Internet of Things</i> (IoT):.....	259
12.1.2 Latar Belakang Tantangan dan Peluang Masa Depan dalam IoT:	259
12.1.3 Tujuan dan Ruang Lingkup Topik:	260
12.2 Tantangan dalam Internet of Things.....	260
12.2.1 Keamanan dan Privasi:	260
12.2.2 Standar dan Kompatibilitas:	261
12.2.3 Keterbatasan Daya dan Sumber Daya:.....	262
12.2.4 Skalabilitas dan Keterhubungan:	262
12.2.5 Regulasi dan Hukum:	263
12.3 Peluang dalam Internet of Things	263
12.3.1 Penyempurnaan Efisiensi Operasional:	263
12.3.2 Pengembangan Produk dan Layanan Baru:.....	264
12.3.3 Analitik Data dan Kecerdasan Buatan (AI):	264
12.3.4 Peningkatan Pengalaman Pengguna:	265
12.4 Perbandingan Tantangan dan Peluang dalam IoT.....	266
12.4.1 Analisis Perbandingan Tantangan dan Peluang: 266	
12.4.2 Strategi Mengatasi Tantangan dan Memanfaatkan Peluang:	267
12.5 Studi Kasus.....	269
12.5.1 Kasus Tantangan dalam Implementasi IoT pada Sektor Industri.	269
12.5.2 Kasus Peluang dalam Penggunaan IoT pada Lingkungan Perkotaan:	269
12.6 Kesimpulan.....	271
12.6.1 Ringkasan Tantangan dan Peluang Masa Depan dalam IoT:	271
12.6.2 Implikasi dan Saran untuk Pengembangan Lebih Lanjut:	272
DAFTAR PUSTAKA	274
BIODATA PENULIS	

DAFTAR GAMBAR

Gambar 2.1. Internet of Things	27
Gambar 4.1. Ilustrasi IoT	65
Gambar 4.2. Ilustrasi IoT Lingkungan.....	69
Gambar 4.3. Ilustrasi IoT dalam Pengelolaan Sumber Daya.....	71
Gambar 4.4. Ilustrasi IoT pada Pertanian Berkelanjutan.....	74
Gambar 4.5. Contoh IoT Pengelolaan Limbah	76
Gambar 4.6. Ilustrasi Iot pada Mobilitas Cerdas	79
Gambar 4.7. Ilustrasi IoT dalam Konversi Energi	82
Gambar 4.8. Ilustrasi IoT dalam Pencegahan Bencana Alam	85
Gambar 4.9. Ilustrasi IoT pada Pendidikan dan Kesadaran Lingkungan	88
Gambar 5.1. Industri 4.0.....	95
Gambar 5.2. Fase-Fase Perkembangan Revolusi Industri.	98
Gambar 5.3. Revolusi Industri.	99
Gambar 5.5. Industrial Internet.....	104
Gambar 5.6. Industrial Internet of Things	108
Gambar 5.7. Cyber-physical systems.....	112
Gambar 7.1. Sistem Pengenalan Aktivitas	149
Gambar 7.2. CNN untuk pengenalan aktivitas manusia	150
Gambar 7.3. Diagram blok sistem deteksi kejang epilepsi.....	152
Gambar 7.4. Monitoring pasien menggunakan Raspberry Pi kit.....	153
Gambar 7.5. Monitoring pasien menggunakan Raspberry Pi kit.....	156
Gambar 7.6. Arduino yang terhubung dengan sensor detak jantung.....	157

Gambar 7.7. Arduino yang terhubung dengan sensor detak jantung dan bluetooth	157
Gambar 7.7. Antarmuka Pengguna (<i>Graphical User Interface - GUI</i>) dari sistem diagnosis sensor detak jantung.....	159
Gambar 7.8. Diagram blok sistem.....	160
Gambar 7.9. K-means clustering untuk segmentasi tumor otak.....	161
Gambar 9.1. IoT Sektor Transportasi.....	201
Gambar 9.2. Proyek transportasi IoT berdasarkan segmen pada tahun 2020.	203
Gambar 9.3. IoT Sektor Transportasi.....	204
Gambar 9.4. Ilustrasi Benefit IoT Transportasi.....	205
Gambar 9.5. Ilustrasi Security pada IoT Kendaraan	206
Gambar 9.6. Ilustrasi Kendaraan Otonom.....	208
Gambar 9.7. Penggunaan IoT Pada Stasiun Pengisian Baterai Kendaraan	209
Gambar 9.8. Ilustrasi Pada Kendaraan Cerdas.....	210
Gambar 9.9. Ilustrasi Pada Kendaraan Cerdas.....	211
Gambar 9.10. Ilustrasi Efisiensi pada Kendaraan Cerdas.....	214
Gambar 9.11. Ilustrasi Pada Kendaraan Cerdas	215
Gambar 9.12. Iot Pada Penggunaan Transportasi Umum Cerdas	216
Gambar 9.13. Ilustrasi Pelacakan Pada Kendaraan	217
Gambar 9.14. Iot Pada Pengaturan GPS pada Kendaraan Cerdas.....	219
Gambar 9.15. IoT dalam Transportasi Logistik	220
Gambar 9.16. Ilustrasi Iot Pada Pengaturan GPS pada Kendaraan Logistik Cerdas.....	221
Gambar 9.17. Alur Informasi IoT pada Transportasi.....	222
Gambar 9.18. Sensor IoT Pada Smart Manajemen <i>Traffic</i>	223
Gambar 9.19. IoT Pendeteksian kendaraan masuk Tol	224

Gambar 9.20. IoT Pelacakan Posisi Kendaraan dan Barang	225
Gambar 9.21. Smart logistik Pengiriman Barang via Drone.....	226
Gambar 10.1. IoT Smart Home	232
Gambar 10.2. Smartphone	234
Gambar 10.3. SmartTV.....	235
Gambar 10.4. Smart Speaker.....	236
Gambar 10.5. Smart Watch.....	236
Gambar 10.7. Home Irrigation	239
Gambar 10.6. Home Security.....	240
Gambar 10.8. Manajemen Energi.....	242
Gambar 10.9. Analitik dan Pengumpulan data	244
Gambar 11.1. Arsitektur IoT IBM(Libow, no date).....	254

DAFTAR TABEL

Tabel 7.1. Fitur normal.....	158
Tabel 7.2. Persamaan untuk untuk ekstraksi fitur (ACO).....	163

BAB 1

PENGANTAR TRANSFORMASI

DIGITAL

Oleh Muhammad Rizal

1.1 Definisi Transformasi Digital

Transformasi digital mengacu pada integrasi teknologi digital ke dalam semua area bisnis dan masyarakat, menghasilkan perubahan mendasar pada cara operasi dan nilai yang diberikan. Bukan hanya tentang mengganti sistem manual dengan yang digital, tetapi juga tentang menggunakan teknologi untuk menciptakan kemungkinan baru dalam cara kita bekerja dan hidup (Hikmah, 2021).

Saat berbicara tentang transformasi digital, banyak yang menganggapnya sebatas tentang otomatisasi proses bisnis atau menerapkan teknologi baru. Namun, lebih dari itu, transformasi ini juga melibatkan perubahan budaya dimana organisasi secara konsisten bereksperimen, menerima gagasan baru, dan menerima kegagalan sebagai bagian dari proses.

Dalam era saat ini, teknologi digital telah menjadi katalis untuk perubahan yang lebih luas. Dengan adanya internet, komputasi awan, analitik data, dan teknologi mobile, batasan antara dunia fisik dan digital semakin kabur. Ini menghasilkan berbagai peluang dan tantangan baru bagi bisnis dan individu.

Definisi transformasi digital tidak hanya terbatas pada bisnis. Sektor-sektor seperti pendidikan, kesehatan, pemerintah, dan lainnya juga mengalami pergeseran mendasar dengan diterapkannya teknologi digital. Misalnya, dalam dunia pendidikan, e-learning dan kelas virtual telah mengubah cara kita mengajar dan belajar.

Dalam konteks bisnis, transformasi digital sering kali berkaitan dengan perubahan model bisnis yang lebih inovatif dan orientasi pelanggan. Teknologi memungkinkan bisnis untuk lebih responsif terhadap kebutuhan dan harapan pelanggan, menciptakan produk dan layanan yang lebih disesuaikan dan personal.

Transformasi digital juga berarti pengumpulan, analisis, dan penggunaan data secara *real-time* untuk mendukung pengambilan keputusan. Dengan kemampuan untuk mengumpulkan data dari berbagai sumber, bisnis dan organisasi sekarang dapat memahami perilaku pelanggan, pasar, dan tren dengan cara yang belum pernah ada sebelumnya (Hadiono and Noor Santi, 2020).

Penting untuk diingat bahwa transformasi digital bukan tujuan akhir, tetapi sebuah perjalanan. Dunia teknologi terus berubah dan berkembang, dan sebagai respons, individu dan organisasi harus terus beradaptasi dan berinovasi.

Untuk menyimpulkan, definisi transformasi digital mencakup berbagai aspek, mulai dari implementasi teknologi hingga perubahan budaya dan struktural dalam organisasi. Ini adalah sebuah revolusi yang menciptakan peluang baru sambil menantang cara lama kita berpikir dan bekerja.

1.2 Evolusi Transformasi Digital

Sebelum era digital, banyak operasi bisnis dan masyarakat berlangsung secara manual, sering kali memerlukan interaksi fisik dan media cetak. Era komputerisasi dimulai pada pertengahan abad ke-20, ketika komputer pertama kali diperkenalkan ke dunia bisnis, merintis jalan untuk otomatisasi tugas-tugas rutin dan peningkatan produktivitas.

Dengan kedatangan internet pada akhir 1990-an dan awal 2000-an, kita melihat sebuah lompatan besar dalam evolusi digital. Internet memungkinkan konektivitas global yang belum pernah ada sebelumnya, mengubah cara kita berkomunikasi, berbelanja,

bekerja, dan bermain. Selain itu, internet menjadi fondasi bagi berbagai inovasi baru, termasuk media sosial, e-commerce, dan aplikasi berbasis cloud.

Era selanjutnya didefinisikan oleh munculnya perangkat mobile seperti smartphone dan tablet. Kemampuan untuk mengakses internet dari hampir mana saja menciptakan gelombang baru inovasi, termasuk aplikasi mobile, layanan berbasis lokasi, dan teknologi berbasis sensor.

Big data dan analitik juga memainkan peran penting dalam evolusi digital. Kemampuan untuk mengumpulkan, menganalisis, dan menarik wawasan dari volume data yang besar memberi perusahaan kesempatan untuk memahami pelanggan dan pasar dengan cara yang lebih mendalam, memungkinkan mereka untuk menyediakan produk dan layanan yang lebih disesuaikan.

Pergeseran ke komputasi awan, di mana data dan aplikasi disimpan di server remote dan diakses melalui internet, memperluas cakupan kemampuan digital dan memberikan fleksibilitas yang belum pernah ada sebelumnya bagi perusahaan untuk mengembangkan dan meningkatkan layanannya.

Internet of Things (IoT) mewakili fase berikutnya dalam evolusi ini. Menghubungkan perangkat sehari-hari, dari kulkas hingga mobil, ke internet menghasilkan data yang dapat dianalisis untuk meningkatkan efisiensi, mengembangkan produk baru, dan menciptakan peluang bisnis yang belum pernah ada sebelumnya (Laurianto, Gracia and Clarissa, 2022).

Kemudian, kecerdasan buatan dan pembelajaran mesin mulai mengambil alih, memberikan perangkat dan sistem kemampuan untuk 'belajar' dari data dan menghasilkan keputusan tanpa intervensi manusia. Hal ini meningkatkan otomatisasi, personalisasi, dan presisi dalam berbagai aplikasi, dari pemasaran hingga diagnosa medis.

Dalam merangkum, evolusi transformasi digital telah melalui berbagai fase, dari komputerisasi awal hingga integrasi AI canggih. Di setiap tahap, teknologi baru menggantikan yang lama,

memperluas kemungkinan dan mengubah cara kita hidup dan bekerja. Ini adalah perjalanan yang terus berlanjut, dengan teknologi baru yang terus muncul dan mempengaruhi dunia kita

1.3 Manfaat Transformasi Digital

Transformasi digital memungkinkan perusahaan untuk menjadi lebih agil dan responsif terhadap perubahan. Dengan teknologi digital, organisasi dapat dengan cepat menyesuaikan strategi dan operasi mereka untuk memenuhi kebutuhan pasar yang berfluktuasi atau mengatasi tantangan yang muncul. Ini menciptakan keunggulan kompetitif dalam lingkungan yang cepat berubah.

Pelanggan saat ini mengharapkan pengalaman yang mulus, cepat, dan disesuaikan dengan kebutuhan mereka. Dengan analisis data yang tepat dan otomatisasi, perusahaan dapat menyediakan pengalaman pelanggan yang lebih personal dan efisien. Ini tidak hanya meningkatkan kepuasan pelanggan, tetapi juga memperkuat loyalitas merek.

Dengan memanfaatkan teknologi digital, perusahaan dapat mengoptimalkan operasi mereka, mengurangi biaya, dan meningkatkan efisiensi. Otomatisasi proses bisnis, contohnya, dapat mengurangi waktu dan sumber daya yang diperlukan untuk tugas-tugas rutin, memungkinkan tim untuk fokus pada inisiatif yang lebih strategis.

Transformasi digital juga mendukung inovasi. Platform dan alat digital memungkinkan tim untuk berkolaborasi dengan lebih efektif, berbagi ide, dan mengembangkan solusi baru untuk masalah yang kompleks. Dengan akses ke data dan analisis, perusahaan dapat mengidentifikasi peluang baru dan menciptakan produk atau layanan yang memenuhi kebutuhan pasar.

Kemampuan untuk mengumpulkan, menganalisis, dan bertindak berdasarkan data dalam waktu nyata adalah salah satu keuntungan paling signifikan dari transformasi digital. Data-driven

decision making memungkinkan organisasi untuk membuat keputusan yang lebih tepat dan proaktif, didasarkan pada wawasan aktual daripada intuisi semata.

Selain itu, transformasi digital membuka pintu untuk pasar global. Bisnis dapat menjangkau audiens yang lebih luas, berinteraksi dengan pelanggan dari berbagai latar belakang geografis, dan memasuki pasar baru dengan biaya yang jauh lebih rendah dibandingkan dengan metode tradisional.

Keamanan dan kepatuhan juga mendapat manfaat dari digitalisasi. Teknologi terbaru dapat memberikan proteksi yang lebih baik terhadap ancaman keamanan siber, sementara otomatisasi dan catatan digital memastikan kepatuhan yang lebih konsisten dengan peraturan dan standar industri.

Secara keseluruhan, manfaat transformasi digital melampaui efisiensi operasional dan mencakup pertumbuhan bisnis, inovasi, kepuasan pelanggan, dan keunggulan kompetitif. Dalam dunia yang semakin digital, penerapan dan adaptasi terhadap teknologi baru adalah kunci untuk kesuksesan jangka panjang.

1.4 Tantangan Transformasi Digital

Meskipun transformasi digital menawarkan sejumlah manfaat, proses transisi dan adaptasi ini juga datang dengan serangkaian tantangan. Salah satu tantangan utama adalah resistensi budaya. Karyawan dan manajemen seringkali terbiasa dengan cara kerja tradisional dan mungkin merasa terancam atau tidak nyaman dengan perubahan yang dibawa oleh teknologi baru.

Keterbatasan teknologi juga menjadi kendala. Menerapkan solusi digital yang tidak sesuai dengan kebutuhan spesifik suatu organisasi atau yang tidak dapat berskala dengan pertumbuhan bisnis dapat mengakibatkan investasi yang sia-sia. Memilih teknologi yang tepat, yang sesuai dengan visi jangka panjang organisasi, adalah kunci.

Keamanan data adalah tantangan lain. Seiring dengan peningkatan konektivitas dan pengumpulan data, risiko pelanggaran keamanan dan pencurian data menjadi semakin nyata. Memastikan keamanan data dan memenuhi peraturan privasi semakin kompleks di era digital.

Keberlanjutan dan pemeliharaan teknologi juga menimbulkan masalah. Seiring dengan perkembangan teknologi, sistem dan aplikasi memerlukan pembaruan dan peningkatan secara reguler. Ini memerlukan investasi waktu dan sumber daya untuk memastikan bahwa teknologi tetap relevan dan efektif.

Selain itu, ada tantangan dalam mengembangkan keterampilan dan pengetahuan yang diperlukan. Pasar kerja saat ini memerlukan keahlian digital yang lebih spesifik. Organisasi sering kali kesulitan menemukan atau melatih karyawan dengan keterampilan yang diperlukan untuk mendukung inisiatif transformasi digital mereka.

Ketidakpastian ROI (Return on Investment) juga menjadi hambatan. Investasi dalam teknologi baru sering kali memerlukan dana yang signifikan, dan tidak selalu jelas kapan dan bagaimana investasi ini akan menghasilkan keuntungan.

Selain itu, integrasi dengan sistem lama bisa menjadi proses yang rumit. Banyak organisasi memiliki infrastruktur IT yang sudah tua dan menggabungkan teknologi baru dengan sistem lama dapat menyebabkan masalah kompatibilitas dan efisiensi.

Terakhir, kecepatan perubahan teknologi memastikan bahwa transformasi digital adalah perjalanan yang berkelanjutan, bukan tujuan. Ini berarti organisasi harus siap untuk beradaptasi, belajar, dan berinovasi secara konstan, yang bisa menjadi tantangan dalam dirinya sendiri.

DAFTAR PUSTAKA

- Hadiono, K. and Noor Santi, R. C. 2020. 'Menyongsong Transformasi Digital', *Proceeding Sendiu*, (July), pp. 978–979. Available at: https://www.researchgate.net/publication/343135526_MENYONGSONG_TRANSFORMASI_DIGITAL.
- Hikmah, N. N. 2021. 'Mengelola transformasi digital', *Jurnal Manajemen dan Bisnis*, 1(1), pp. 1–4.
- Laurianto, E., Gracia, E. and Clarissa, F. 2022. 'Transformasi Peternakan Digital dengan Mengimplementasikan Teknologi Internet of Things (IoT) pada Arjuna Farm', *Jurnal Pengabdian kepada Masyarakat Nusantara*, 3(1), pp. 300–308. Available at: <http://ejournal.sisfokomtek.org/index.php/jpkm/article/view/329>.

BAB 2

KONSEP DASAR INTERNET OF THINGS

Oleh Arief Yanto Rukmana

2.1 Pendahuluan

Internet of Things (IoT) mengacu pada jaringan benda fisik, perangkat, dan sensor yang saling terhubung yang dapat mengumpulkan dan bertukar data melalui internet tanpa perlu campur tangan manusia secara langsung (Khari *et al.*, 2016). Konsep dasar IoT adalah memungkinkan perangkat untuk berkomunikasi satu sama lain dan dengan server pusat (An, Gui and He, 2012), menciptakan ekosistem luas dari "benda" yang saling berhubungan (Sunyaev and Sunyaev, 2020).

Inti dari IoT adalah "benda" itu sendiri, yang dapat berupa apa saja mulai dari benda sehari-hari (Sunyaev and Sunyaev, 2020) seperti jam tangan pintar, termostat, dan peralatan rumah tangga, hingga peralatan dan infrastruktur industri seperti sensor di pabrik atau sistem kota pintar (Dongsheng *et al.*, 2019). Perangkat ini disematkan dengan sensor dan modul komunikasi yang memungkinkan mengumpulkan dan mengirimkan data tentang lingkungan atau status sendiri (Yue *et al.*, 2015).

Konektivitas adalah aspek penting dari IoT, memungkinkan pertukaran data yang mulus antara perangkat dan sistem pusat. Perangkat IoT menggunakan berbagai teknologi komunikasi, seperti Wi-Fi, jaringan seluler, Bluetooth, Zigbee, dan LoRaWAN, untuk terhubung ke internet dan perangkat lainnya (Cao *et al.*, 2019). Konektivitas ini memungkinkan pengiriman data dari sensor secara real-time, memfasilitasi pengambilan keputusan

yang cepat dan memungkinkan pemantauan dan kontrol jarak jauh (Sun, Liu and Li, 2010).

Data yang dikumpulkan oleh perangkat IoT adalah sumber kehidupan ekosistem IoT. Perangkat ini menghasilkan sejumlah besar data dari berbagai sumber, seperti suhu, kelembapan, gerakan, lokasi, dan lainnya. Data ini dapat terstruktur, semi-terstruktur, atau tidak terstruktur, dan memberikan wawasan berharga yang dapat dimanfaatkan untuk analisis dan pengambilan keputusan (Xiaohui, 2013).

Arsitektur IoT memainkan peran penting dalam mengatur dan mengelola aliran data dalam ekosistem IoT. Arsitektur biasanya terdiri dari lapisan, termasuk lapisan Persepsi, lapisan Jaringan, lapisan Pemrosesan Data, dan lapisan Aplikasi (Çorak *et al.*, 2018). Lapisan Persepsi melibatkan sensor dan perangkat yang mengumpulkan data dari dunia fisik. Lapisan Jaringan menangani transmisi data dan komunikasi, sedangkan lapisan Pemrosesan Data memproses dan menganalisis data untuk mengekstrak wawasan yang berharga (Gerodimos *et al.*, 2023). Lapisan Aplikasi memungkinkan pengguna akhir untuk berinteraksi dengan data dan membuat keputusan berdasarkan informasi yang diproses (Ukil, Sen and Koilakonda, 2011).

Potensi transformatif IoT terletak pada kemampuannya untuk mengaktifkan otomatisasi dan pengambilan keputusan berbasis data (Lavric and Petrariu, 2018). Dengan memanfaatkan analitik data IoT, bisnis dapat mengoptimalkan proses, meningkatkan efisiensi, dan menciptakan pengalaman pengguna yang dipersonalisasi (Rozi, 2020). Misalnya, di rumah pintar, perangkat IoT dapat mempelajari preferensi pengguna dan menyesuaikan pengaturan suhu, pencahayaan, dan sistem hiburan secara otomatis, sehingga meningkatkan kenyamanan dan efisiensi energi (Davies and Fortuna, 2020).

Sementara IoT menghadirkan peluang yang luar biasa, itu juga menimbulkan tantangan yang signifikan. Keamanan adalah perhatian utama, karena perangkat yang terhubung dapat rentan

terhadap serangan dunia maya dan akses tidak sah (Moraes *et al.*, 2019). Memastikan keamanan perangkat yang kuat, enkripsi data, dan protokol komunikasi yang aman sangat penting untuk melindungi ekosistem IoT dari potensi ancaman (Tripathy and Anuradha, 2017).

Skala besar dan keragaman perangkat IoT dapat menyebabkan masalah interoperabilitas dan manajemen data. Standarisasi di seluruh industri dan protokol terbuka sangat penting untuk memastikan komunikasi yang mulus antara berbagai perangkat dan platform (Abdel-Basset *et al.*, 2019).

Konsep dasar Internet of Things berputar di sekitar interkoneksi perangkat dan kemampuan untuk mengumpulkan, mengirim, dan menganalisis data untuk mendorong otomatisasi dan pengambilan keputusan yang terinformasi (Song *et al.*, 2017). IoT memiliki potensi untuk merevolusi industri, meningkatkan kualitas hidup, dan membentuk kembali cara kita berinteraksi dengan teknologi. Sementara ada tantangan, mengatasi masalah keamanan, interoperabilitas, dan privasi data akan menjadi sangat penting dalam membuka potensi penuh IoT dan mewujudkan dampak transformatifnya di berbagai domain (Liu and Zhou, 2012).

2.2 Memahami Dasar-Dasar IoT

Dasar-dasar *Internet of Things* (IoT) membentuk landasan teknologi transformatif ini yang membentuk kembali lanskap digital (Ma, 2011). Untuk memahami esensi IoT, sangat penting untuk mempelajari latar belakang sejarah dan evolusinya (Jabraeil Jamali *et al.*, 2020). IoT telah muncul dari konvergensi berbagai teknologi, termasuk sistem tertanam, komunikasi nirkabel, dan komputasi awan. Ini telah berkembang dari konsep perangkat interkoneksi ke ekosistem canggih yang mendorong pengambilan keputusan dan otomatisasi berbasis data (Wilianto and Kurniawan, 2018).

Pada intinya, IoT dibangun di atas kombinasi komponen penting yang bekerja secara harmonis untuk memungkinkan konektivitas tanpa batas dan pertukaran data. Perangkat dan sensor memainkan peran penting dalam sistem IoT, karena berfungsi sebagai antarmuka fisik antara dunia nyata dan dunia digital. Perangkat ini dilengkapi dengan sensor yang dapat menangkap dan mengukur data dari lingkungan, baik itu suhu, kelembapan, gerakan, atau parameter lain yang relevan. Data ini kemudian ditransmisikan menggunakan berbagai teknologi konektivitas, seperti Wi-Fi, jaringan seluler, atau protokol berdaya rendah seperti Zigbee dan LoRaWAN, yang membentuk lapisan jaringan.

Setelah mencapai lapisan pemrosesan data, informasi yang dikumpulkan mengalami pemrosesan dan analisis penting. Lapisan ini terdiri dari sumber daya komputasi yang kuat dan algoritme yang bertanggung jawab atas agregasi data, pemfilteran, dan ekstraksi wawasan yang berharga. Selain itu, platform berbasis cloud memainkan peran penting dalam menyimpan dan mengelola sejumlah besar data yang dihasilkan oleh perangkat IoT. Data kemudian tersedia untuk aplikasi yang berjalan di lapisan aplikasi, memungkinkan pengguna untuk berinteraksi dengan ekosistem IoT melalui antarmuka intuitif dan mengekstrak informasi berharga untuk pengambilan keputusan.

Protokol komunikasi sangat penting untuk IoT, memungkinkan pertukaran data yang efisien dan aman antara perangkat dan cloud. MQTT, CoAP, HTTP/HTTPS, Bluetooth, dan Zigbee adalah beberapa protokol umum yang digunakan untuk memfasilitasi komunikasi tanpa batas. Untuk membuka potensi sebenarnya dari IoT, analitik data memegang peran penting. Ini mencakup berbagai teknik seperti analitik deskriptif, prediktif, dan preskriptif, yang memproses data untuk memperoleh pola, tren, dan prediksi yang bermakna (Tripathy and Anuradha, 2017). Informasi ini sangat penting bagi bisnis dan industri untuk

mengoptimalkan proses, meningkatkan efisiensi, dan mendapatkan keunggulan kompetitif (Liu and Zhou, 2012).

Seperti halnya teknologi apa pun, IoT hadir dengan tantangannya sendiri, terutama terkait keamanan dan privasi. Perangkat IoT, yang sering digunakan di lingkungan terpencil dan rentan, rentan terhadap serangan dunia maya. Memastikan keamanan perangkat yang kuat, keamanan jaringan, dan keamanan data sangat penting untuk melindungi dari potensi ancaman. Selain itu, masalah privasi muncul karena banyaknya data pribadi dan sensitif yang dihasilkan oleh perangkat IoT. Menerapkan langkah-langkah privasi dan mematuhi persyaratan peraturan diperlukan untuk membangun kepercayaan di antara pengguna dan konsumen.

Penerapan IoT di era transformasi digital sangat luas dan berjangkauan luas. Kota pintar memanfaatkan IoT untuk meningkatkan infrastruktur perkotaan, mengoptimalkan pengelolaan sumber daya, dan meningkatkan kualitas hidup penduduk. Sektor industri merangkul Industrial IoT (IIoT) untuk merampingkan proses manufaktur, memantau kesehatan mesin, dan mencapai tingkat efisiensi dan produktivitas yang belum pernah terjadi sebelumnya di Industri 4.0. Dampak IoT dalam perawatan kesehatan sangat signifikan, dengan perangkat medis yang terhubung memungkinkan pemantauan pasien jarak jauh, perawatan yang dipersonalisasi, dan hasil perawatan kesehatan yang lebih baik. Demikian pula, IoT menemukan aplikasi di bidang pertanian, transportasi, dan logistik, merevolusi sektor-sektor ini melalui peningkatan otomatisasi dan wawasan berbasis data.

Melihat ke masa depan, pertumbuhan IoT tidak menunjukkan tanda-tanda melambat. Seiring kemajuan teknologi, IoT kemungkinan akan menyaksikan inovasi dan transformasi lebih lanjut. Dari edge computing hingga konektivitas 5G, tren yang muncul memiliki potensi untuk membentuk kembali lanskap IoT. Namun, seiring berkembangnya ekosistem IoT, tantangan yang berkaitan dengan standarisasi, interoperabilitas, dan tata kelola

data akan memerlukan pertimbangan yang cermat. Merangkul pendekatan yang bertanggung jawab dan etis akan sangat penting dalam membuka potensi penuh IoT sambil memitigasi potensi risiko (Cheng *et al.*, 2022).

Memahami dasar-dasar IoT sangat penting dalam menavigasi seluk-beluk teknologi transformatif ini. Dari akar historis hingga komponen intinya, IoT menawarkan peluang tak tertandingi untuk bisnis, industri, dan Masyarakat (Sharma and Gondhi, 2018). Dengan memanfaatkan kekuatan konektivitas, analitik data, dan komunikasi yang aman, IoT siap membentuk masa depan dunia digital, mendorong inovasi, dan mendorong kita menuju masa depan yang lebih terhubung dan cerdas (Wilianto and Kurniawan, 2018).

2.3 Arsitektur IoT

Arsitektur *Internet of Things* (IoT) berfungsi sebagai cetak biru untuk membangun dan menerapkan sistem IoT (Meutia, 2015). Ini menguraikan struktur dan organisasi berbagai komponen, memungkinkan integrasi perangkat, jaringan, dan pemrosesan data tanpa batas (Rukmana *et al.*, 2023). Memahami arsitektur IoT sangat penting untuk merancang solusi IoT yang dapat diskalakan, efisien, dan aman (Rozi, 2020).

Pada tingkat tinggi, arsitektur IoT terdiri dari empat lapisan utama: lapisan Persepsi, lapisan Jaringan, lapisan Pemrosesan Data, dan lapisan Aplikasi (Mulyana *et al.*, 2019). Lapisan Persepsi adalah titik masuk IoT, tempat sensor dan perangkat berinteraksi dengan dunia fisik, mengumpulkan data dari lingkungan (Setiaji, Sofwan and Sumardi, 2019). Sensor ini dapat mengukur berbagai parameter, seperti suhu, tekanan, kelembapan, dan gerakan, mengubah peristiwa dunia nyata menjadi data digital (Jabraeil Jamali *et al.*, 2020).

Lapisan Jaringan bertanggung jawab untuk mentransmisikan data yang dikumpulkan dari lapisan Persepsi ke

cloud atau server terpusat untuk diproses lebih lanjut. Lapisan ini mencakup berbagai protokol dan teknologi komunikasi yang memastikan transmisi data yang andal dan aman. Protokol komunikasi yang umum digunakan di IoT termasuk MQTT, CoAP, HTTP/HTTPS, Bluetooth, Zigbee, dan LoRaWAN, masing-masing melayani kasus dan persyaratan penggunaan tertentu (Al-Qaseemi *et al.*, 2016).

Setelah data mencapai lapisan Pemrosesan Data, data tersebut mengalami pemrosesan dan analisis penting. Lapisan ini melibatkan sumber daya komputasi yang canggih, sering dihosting di platform berbasis cloud (Sunyaev and Sunyaev, 2020). Teknik pemrosesan data seperti pemfilteran, agregasi, dan pengenalan pola diterapkan pada data yang masuk untuk mendapatkan wawasan yang berharga (Lloret *et al.*, 2016). Dalam beberapa kasus, komputasi tepi digunakan untuk melakukan pemrosesan data lebih dekat ke sumber data, mengurangi latensi, dan menghemat bandwidth (Krčo, Pokrić and Carrez, 2014).

Data yang diproses kemudian tersedia di lapisan Aplikasi, di mana data tersebut dapat diakses oleh pengguna akhir atau aplikasi untuk visualisasi, pemantauan, dan pengambilan keputusan. Lapisan Aplikasi menyediakan berbagai antarmuka di mana pengguna dapat berinteraksi dengan ekosistem IoT, mulai dari dasbor berbasis web hingga aplikasi seluler. Lapisan ini memungkinkan bisnis, industri, dan konsumen untuk memperoleh informasi yang berarti dari data yang dikumpulkan dan mengambil tindakan yang sesuai (Gupta and Quamara, 2020).

Arsitektur IoT sangat fleksibel dan dapat disesuaikan untuk memenuhi kebutuhan spesifik dari berbagai aplikasi dan industri. Misalnya, dalam skenario Industrial IoT (IIoT), arsitektur mungkin melibatkan pendekatan hybrid, menggabungkan edge computing untuk pemrosesan data real-time dan platform berbasis cloud untuk penyimpanan dan analitik data jangka panjang (Moraes *et al.*, 2019). Di sisi lain, dalam aplikasi IoT konsumen, arsitekturnya mungkin lebih terfokus pada antarmuka yang ramah pengguna dan

integrasi tanpa batas dengan perangkat pintar (Kumar, Tiwari and Zymbler, 2019).

Keamanan adalah aspek penting dari arsitektur IoT. Karena perangkat IoT sering beroperasi di lingkungan yang tidak terkendali, IoT rentan terhadap serangan dunia maya. Memastikan tindakan keamanan yang kuat di setiap lapisan arsitektur sangat penting untuk melindungi data sensitif dan mencegah akses tidak sah (Rozi, 2020). Mekanisme keamanan dapat mencakup enkripsi, autentikasi, kontrol akses, dan pembaruan perangkat lunak reguler untuk menambal kerentanan (Zhong, Zhu and Huang, 2015).

Arsitektur IoT berfungsi sebagai dasar untuk menciptakan sistem IoT yang saling berhubungan dan cerdas. Ini memfasilitasi aliran data yang mulus dari perangkat ke aplikasi, memungkinkan wawasan waktu nyata dan pengambilan keputusan berdasarkan data (Ganchev, Ji and O'Droma, 2014). Dengan memahami berbagai lapisan dan fungsinya, pengembang dan organisasi dapat merancang dan mengimplementasikan solusi IoT yang tangguh dan aman yang mendorong inovasi dan meningkatkan efisiensi di berbagai industri dan domain (Lloret *et al.*, 2016). Saat IoT terus berkembang, kemajuan dalam teknologi dan standar akan membentuk masa depan arsitektur IoT, membuka kemungkinan baru untuk dunia yang lebih cerdas dan lebih terhubung (Oesterreich, Anton and Teuteberg, 2022).

2.4 Protokol Komunikasi IoT

Protokol komunikasi IoT memainkan peran penting dalam memungkinkan pertukaran data yang mulus dan efisien antara perangkat yang terhubung dan cloud (Dizdarević *et al.*, 2019). Ketika Internet of Things terus berkembang (Song *et al.*, 2017), berbagai protokol komunikasi telah muncul, masing-masing disesuaikan dengan kasus penggunaan, persyaratan, dan kendala tertentu (Al-Sarawi *et al.*, 2017).

Salah satu protokol komunikasi IoT yang paling banyak digunakan adalah MQTT (*Message Queuing Telemetry Transport*). MQTT dikenal dengan desainnya yang ringan dan efisien, menjadikannya ideal untuk perangkat berdaya rendah dan jaringan terbatas. Ini mengikuti pola terbitkan-berlangganan, di mana perangkat menerbitkan data ke broker, dan perangkat atau aplikasi lain berlangganan ke topik tertentu untuk menerima data yang di butuhkan. Model komunikasi terpisah ini memungkinkan transmisi data secara real-time dan mengurangi dampak pada bandwidth jaringan (Çorak *et al.*, 2018).

CoAP (*Constrained Application Protocol*) adalah protokol komunikasi IoT populer lainnya, yang dirancang khusus untuk perangkat dan jaringan dengan sumber daya terbatas. CoAP dibangun di atas UDP, menjadikannya ringan dan cocok untuk penerapan IoT di lingkungan yang terbatas. Ini menawarkan model komunikasi permintaan-respons, mirip dengan HTTP, yang memungkinkan perangkat untuk berinteraksi dengan sumber daya pada perangkat atau server lain menggunakan metode GET, PUT, POST, dan DELETE sederhana (Song *et al.*, 2017).

HTTP (*Hypertext Transfer Protocol*) dan versi amannya, HTTPS, adalah protokol komunikasi IoT yang umum digunakan. Mereka memanfaatkan infrastruktur internet yang ada, membuatnya mudah diimplementasikan dan didukung secara luas. Namun, HTTP/HTTPS mungkin bukan pilihan terbaik untuk perangkat IoT dengan sumber daya terbatas karena overhead yang relatif lebih tinggi dibandingkan dengan MQTT dan CoAP. Namun demikian, banyak digunakan dalam aplikasi IoT yang memerlukan interoperabilitas dengan layanan web tradisional (Gerodimos *et al.*, 2023).

Bluetooth dan *Bluetooth Low Energy* (BLE) adalah protokol komunikasi IoT yang lazim untuk komunikasi nirkabel jarak pendek antar perangkat. Mereka umumnya digunakan dalam aplikasi IoT konsumen seperti perangkat yang dapat dikenakan, perangkat rumah pintar, dan pelacak kesehatan pribadi. BLE,

khususnya, dioptimalkan untuk konsumsi daya yang rendah, sehingga cocok untuk perangkat yang dioperasikan dengan baterai yang perlu beroperasi dalam waktu lama.

Zigbee adalah protokol komunikasi IoT jaringan mesh yang dirancang untuk aplikasi berdaya rendah dan laju data rendah. Perangkat yang mendukung Zigbee dapat membentuk jaringan mesh penyembuhan sendiri, memungkinkan komunikasi yang kuat dan andal bahkan dalam penerapan skala besar. Ini biasanya digunakan dalam otomatisasi rumah pintar, pemantauan industri, dan otomatisasi bangunan (Moraes *et al.*, 2019).

LoRaWAN (*Long Range Wide Area Network*) adalah protokol komunikasi IoT yang dioptimalkan untuk komunikasi jarak jauh dengan perangkat berdaya rendah yang dioperasikan dengan baterai. LoRaWAN beroperasi dalam spektrum tanpa lisensi, sehingga cocok untuk penerapan area luas di kota pintar, pertanian, dan pemantauan lingkungan (Lavric and Petrariu, 2018).

Setiap protokol komunikasi IoT memiliki kekuatan dan kelemahannya masing-masing, dan pilihan protokol bergantung pada persyaratan khusus dari aplikasi IoT. Faktor-faktor seperti konsumsi daya, kecepatan data, jangkauan, topologi jaringan, dan interoperabilitas perlu dipertimbangkan saat memilih protokol yang sesuai (Rozi, 2020). Selain itu, keamanan adalah pertimbangan penting dalam komunikasi IoT. Menerapkan enkripsi, autentikasi, dan transmisi data yang aman sangat penting untuk melindungi informasi sensitif dan memastikan integritas dan privasi sistem IoT. Saat IoT terus berkembang, protokol dan standar komunikasi baru akan muncul, berkontribusi pada pertumbuhan dan kemajuan teknologi transformatif ini (Dong and Yang, 2020).

2.5 Analisis Data IoT

IoT Data Analytics adalah aspek penting dari ekosistem Internet of Things (Mikalef *et al.*, 2019), di mana sejumlah besar data dihasilkan oleh perangkat yang saling terhubung (Vitari and Raguseo, 2020). Tujuan utama analitik data IoT adalah untuk mengekstrak wawasan berharga dan pola bermakna dari data ini untuk mendorong pengambilan keputusan yang tepat dan mengoptimalkan proses (Ferraris *et al.*, 2019).

Analitik data IoT mencakup berbagai teknik yang membantu mengubah data mentah menjadi informasi yang dapat ditindaklanjuti. Analitik deskriptif adalah langkah pertama, yang melibatkan peringkasan dan visualisasi data historis (Ardito *et al.*, 2019). Teknik ini memungkinkan bisnis dan organisasi untuk mendapatkan ikhtisar peristiwa dan tren masa lalu, memberikan landasan untuk analisis lebih lanjut (Ngiam and Khor, 2019).

Analitik prediktif membawa analitik data IoT selangkah lebih maju dengan menggunakan data historis untuk memperkirakan tren dan hasil di masa mendatang. Dengan menggunakan algoritme pembelajaran mesin, analitik prediktif dapat mengidentifikasi pola dan korelasi dalam data, memungkinkan prediksi potensi masalah, anomali, atau peluang (Ageed *et al.*, 2021).

Analitik preskriptif adalah analitik data IoT tingkat tertinggi, yang bertujuan untuk memberikan rekomendasi dan saran yang dapat ditindaklanjuti berdasarkan wawasan yang diperoleh dari analitik deskriptif dan prediktif (Lalit *et al.*, 2022). Tingkat analisis ini membantu pembuat keputusan dalam memahami tindakan terbaik untuk mengoptimalkan proses, meningkatkan efisiensi, dan meningkatkan kinerja (Sadhu, Yanambaka and Abdelgawad, 2022).

Berbagai alat dan teknologi digunakan dalam analitik data IoT. Platform Big Data digunakan untuk menyimpan dan memproses data dalam volume besar yang dihasilkan oleh perangkat IoT (Baig, Shuib and Yadegaridehkordi, 2019). Platform

ini dapat menangani beragam tipe data, termasuk data terstruktur, semi-terstruktur, dan tidak terstruktur, memfasilitasi pemrosesan data dalam skala besar (VARGA and KUJUNDZIC, 2022).

Algoritme pembelajaran mesin memainkan peran penting dalam analitik data IoT, memungkinkan deteksi pola secara otomatis, klasifikasi data, dan prediksi kejadian di masa mendatang. Model pembelajaran mesin dapat dilatih untuk mengenali anomali atau memprediksi kegagalan peralatan, membantu bisnis menerapkan strategi pemeliharaan proaktif (Samaila *et al.*, 2017).

Alat visualisasi data digunakan untuk menyajikan hasil analitik data IoT dengan cara yang ramah pengguna dan mudah dipahami. Dengan menggunakan grafik, bagan, dan dasbor, pemangku kepentingan dapat memperoleh wawasan dari kumpulan data yang kompleks tanpa memerlukan pengetahuan teknis khusus.

Analitik tepi adalah tren yang muncul dalam analitik data IoT. Alih-alih mengirimkan semua data ke cloud untuk diproses, analitik tepi melibatkan pelaksanaan analisis data di tepi jaringan, lebih dekat ke sumber data. Pendekatan ini mengurangi latensi, menghemat bandwidth, dan memungkinkan pengambilan keputusan secara real-time (Mughal, 2022).

Analitik data IoT menemukan aplikasi ekstensif di berbagai industri. Di bidang manufaktur, analitik prediktif membantu mengoptimalkan proses produksi, mengurangi waktu henti, dan meningkatkan efisiensi. Dalam perawatan kesehatan, analitik data membantu pemantauan pasien jarak jauh dan rencana perawatan yang dipersonalisasi. Di kota pintar, analitik memungkinkan pengelolaan sumber daya yang efisien dan meningkatkan layanan perkotaan (Ukil, Sen and Koilakonda, 2011).

Keamanan dan privasi adalah pertimbangan penting dalam analitik data IoT. Karena data dikumpulkan dari banyak perangkat dan sensor, memastikan integritas data dan melindungi informasi sensitif adalah hal yang terpenting. Menerapkan enkripsi yang kuat

dan kontrol akses sangat penting untuk melindungi data dari akses yang tidak sah (Yathiraju *et al.*, 2022).

Analitik data IoT memberdayakan organisasi untuk memperoleh wawasan berharga dari sejumlah besar data yang dihasilkan oleh perangkat IoT. Teknik analitik deskriptif, prediktif, dan preskriptif memberikan pendekatan komprehensif untuk memahami tren data historis, sekarang, dan masa depan. Dengan memanfaatkan alat dan teknologi canggih, bisnis dapat mengoptimalkan proses, membuat keputusan berdasarkan informasi, dan membuka potensi penuh ekosistem IoT di berbagai industri dan kasus penggunaan. Seiring lanskap IoT terus berkembang, analitik data akan tetap menjadi landasan dalam mendorong inovasi dan perubahan transformatif (Davies and Price, 1984).

2.6 Keamanan dan Privasi IoT

Keamanan dan Privasi IoT adalah aspek penting dari ekosistem *Internet of Things*, karena sifat perangkat IoT yang saling terhubung menghadirkan tantangan dan kerentanan yang unik (Bishop, 2004). Memastikan langkah-langkah keamanan yang kuat dan melindungi privasi pengguna sangat penting untuk membangun kepercayaan dan mendorong adopsi teknologi IoT secara luas (Choubey *et al.*, 2022).

Salah satu perhatian utama dalam keamanan IoT adalah perlindungan perangkat itu sendiri. Perangkat IoT sering digunakan di lingkungan yang tidak terkontrol dan mungkin tidak memiliki fitur keamanan yang memadai. Ini membuat rentan terhadap serangan dunia maya dan potensi eksploitasi oleh aktor jahat. Menerapkan langkah-langkah keamanan tingkat perangkat, seperti boot aman, pembaruan firmware, dan autentikasi berbasis perangkat keras, sangat penting untuk melindungi dari akses dan gangguan yang tidak sah (Novianto, Ujianto and Rianto, 2023).

Keamanan jaringan adalah aspek penting lain dari keamanan IoT. Karena perangkat IoT berkomunikasi satu sama lain dan dengan layanan cloud melalui berbagai jaringan, mengamankan saluran komunikasi sangatlah penting. Protokol enkripsi, seperti SSL/TLS, memastikan bahwa data yang dikirimkan antara perangkat dan server terlindung dari penyadapan dan perusakan. Selain itu, menerapkan protokol komunikasi yang aman, seperti MQTT dengan nama pengguna/sandi atau sertifikat klien, membantu mengurangi risiko intersepsi data dan akses tidak sah.

Keamanan data sangat penting dalam IoT, mengingat banyaknya data yang dihasilkan dan dipertukarkan antara perangkat dan cloud. Enkripsi data selama transmisi dan penyimpanan membantu melindungi informasi sensitif agar tidak disusupi. Anonimisasi data dan teknik agregasi juga dapat digunakan untuk mengurangi risiko data individu ditelusuri kembali ke pengguna tertentu, menjaga privasi pengguna (Wang *et al.*, 2022).

Prinsip "keamanan berdasarkan desain" sangat penting dalam pengembangan IoT. Pendekatan ini melibatkan penggabungan langkah-langkah keamanan di setiap tahap siklus hidup perangkat IoT, mulai dari desain dan pengembangan hingga penerapan dan penonaktifan. Melakukan penilaian keamanan menyeluruh dan mematuhi standar industri dan praktik terbaik sangat penting untuk mengidentifikasi dan mengatasi potensi kerentanan di awal proses pengembangan (Setiawan *et al.*, 2023).

Perangkat IoT sering kali memiliki daya komputasi dan memori yang terbatas, yang dapat mempersulit penerapan keamanan yang kuat. Namun, kemajuan dalam modul keamanan perangkat keras dan algoritme enkripsi yang ringan memungkinkan penerapan keamanan yang efisien bahkan pada perangkat dengan sumber daya terbatas (Rijal *et al.*, 2023).

Perangkat IoT sering mengumpulkan dan memproses data pribadi, menimbulkan kekhawatiran tentang kepemilikan dan

penggunaan data. Menerapkan prinsip privasi per desain dan memberikan kebijakan privasi yang transparan dapat membantu membangun kepercayaan dan keyakinan pengguna dalam teknologi IoT (Sutaguna *et al.*, 2023). Kepatuhan peraturan merupakan pertimbangan penting dalam keamanan dan privasi IoT. Bergantung pada wilayah geografis dan sifat data yang dikumpulkan, organisasi mungkin perlu mematuhi berbagai peraturan perlindungan data dan privasi, seperti GDPR (Peraturan Perlindungan Data Umum) di Uni Eropa.

Pemantauan dan pembaruan berkelanjutan sangat penting untuk menjaga keamanan IoT. Saat ancaman berkembang, tambalan dan pembaruan keamanan harus segera digunakan untuk mengatasi setiap kerentanan yang baru teridentifikasi. Audit keamanan reguler dan penilaian kerentanan membantu memastikan ekosistem IoT tetap kuat dan tangguh terhadap potensi serangan.

Keamanan dan privasi IoT sangat penting dalam membangun ekosistem IoT yang tepercaya dan tangguh. Keamanan perangkat, keamanan jaringan, dan tindakan keamanan data, bersama dengan prinsip privasi per desain, merupakan komponen penting dari strategi keamanan yang komprehensif (Dongsheng *et al.*, 2019). Dengan menggabungkan langkah-langkah keamanan di setiap tingkat pengembangan IoT dan mematuhi praktik terbaik dan persyaratan peraturan, organisasi dapat mengembangkan lingkungan yang aman dan terlindungi untuk penerapan IoT, mendorong inovasi, dan memungkinkan potensi penuh teknologi IoT (Yue *et al.*, 2015).

2.7 Aplikasi IoT dalam Transformasi Digital

Penerapan IoT dalam transformasi digital sangat luas dan berdampak, merevolusi industri dan meningkatkan cara kita hidup dan bekerja (Pamarthi and Narmadha, 2022). Kemampuan IoT untuk menghubungkan dan mengumpulkan data dari berbagai

perangkat dan lingkungan memungkinkan terciptanya sistem cerdas berbasis data yang mengoptimalkan proses, meningkatkan efisiensi, dan meningkatkan pengalaman pengguna (Shalaginov, Iqbal and Olegård, 2020).

Salah satu penerapan IoT yang menonjol dalam transformasi digital adalah di Kota Cerdas (An, Gui and He, 2012). Dengan menerapkan sensor dan perangkat berkemampuan IoT di seluruh area perkotaan, kota dapat mengumpulkan data real-time tentang lalu lintas, kualitas udara, pengelolaan limbah, dan konsumsi energi (Kyriakakis, Sparsø and Schoeberl, 2019). Data ini memungkinkan pemerintah kota membuat keputusan untuk mengoptimalkan alokasi sumber daya, mengurangi kemacetan lalu lintas, dan meningkatkan kelestarian lingkungan. Penerangan jalan pintar yang diaktifkan IoT, misalnya, dapat menyesuaikan tingkat pencahayaan berdasarkan pola lalu lintas waktu nyata, mengurangi konsumsi energi, dan meningkatkan keselamatan (Kyriakakis, Sparsø and Schoeberl, 2019; Rukmana, 2023).

Di sektor industri, IoT mendorong munculnya Industri 4.0 dan Industrial IoT (IIoT). Dengan melengkapi peralatan manufaktur dan mesin dengan sensor IoT, pabrik dapat melakukan pemantauan real-time dan pemeliharaan prediktif. Analitik data yang diperoleh dari sensor ini dapat memberikan wawasan tentang kesehatan dan kinerja peralatan, membantu menghindari waktu henti yang tidak direncanakan dan meningkatkan produktivitas secara keseluruhan. IIoT juga memfasilitasi komunikasi dan kolaborasi yang mulus di antara berbagai komponen proses produksi, yang menghasilkan rantai pasokan yang lebih efisien dan operasi yang disederhanakan.

IoT memainkan peran penting dalam industri perawatan kesehatan, memungkinkan konsep pemantauan pasien jarak jauh. Perangkat medis dan perangkat yang dapat dikenakan dengan IoT dapat terus mengumpulkan dan mengirimkan tanda-tanda vital dan metrik kesehatan ke penyedia layanan kesehatan. Data ini memberdayakan dokter untuk memantau kondisi kesehatan

pasien dari jarak jauh dan melakukan intervensi segera bila diperlukan, meningkatkan hasil pasien dan mengurangi beban fasilitas kesehatan. Selain itu, solusi telemedis bertenaga IoT memungkinkan konsultasi virtual dan diagnosis jarak jauh, memperluas akses ke layanan kesehatan, terutama di daerah terpencil atau kurang terlayani (Thangaramya *et al.*, 2019).

Di bidang pertanian, IoT mengubah praktik pertanian tradisional menjadi pertanian presisi. Sensor IoT di lapangan dapat memantau kelembapan tanah, suhu, dan tingkat nutrisi, memungkinkan petani membuat keputusan berbasis data terkait irigasi dan pemupukan. Drone yang dilengkapi sensor IoT dapat mensurvei lahan pertanian yang luas, mengidentifikasi area yang membutuhkan perhatian, bahkan mendistribusikan benih atau pestisida dengan tepat. Sistem irigasi pintar bertenaga IoT mengoptimalkan penggunaan air, yang mengarah pada peningkatan hasil panen dan konservasi sumber daya.

Dampak IoT meluas ke transportasi dan logistik, di mana kendaraan yang terhubung dan solusi logistik pintar meningkatkan efisiensi dan keamanan. Sensor IoT di kendaraan dapat memantau kinerja mesin, konsumsi bahan bakar, dan perilaku pengemudi, yang menghasilkan perawatan proaktif dan pengurangan biaya bahan bakar. Dalam logistik, IoT memungkinkan pelacakan dan pemantauan pengiriman secara real-time, memastikan manajemen rantai pasokan yang efisien dan mengurangi risiko barang hilang atau rusak.

Rumah pintar dan aplikasi IoT konsumen menjadi semakin populer, membuat kehidupan sehari-hari lebih nyaman dan hemat energi. Perangkat rumah pintar berkemampuan IoT, seperti termostat pintar, pencahayaan pintar, dan peralatan pintar, dapat dikontrol dari jarak jauh melalui aplikasi smartphone atau perintah suara. Tingkat otomatisasi dan kontrol ini memungkinkan pengguna mengoptimalkan penggunaan energi, meningkatkan keamanan rumah, dan menciptakan lingkungan hidup yang dipersonalisasi (Kumar *et al.*, 2021).

Penerapan IoT dalam transformasi digital sangatlah luas dan beragam, menyentuh hampir setiap aspek kehidupan modern. Dengan memanfaatkan kekuatan perangkat yang terhubung, analitik data, dan wawasan real-time, IoT memberdayakan industri dan individu untuk membuat keputusan yang lebih cerdas dan berdasarkan data. Seiring dengan perkembangan teknologi, dampak IoT pada transformasi digital diperkirakan akan tumbuh, membuka kemungkinan dan peluang baru untuk inovasi di berbagai sektor dan domain (Choubey *et al.*, 2022).

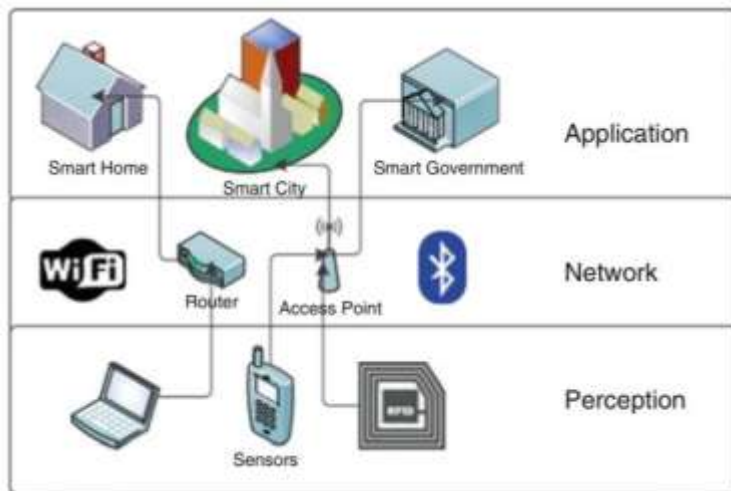
2.8 Tren dan Tantangan Masa Depan IoT

Masa depan IoT sangat menjanjikan karena teknologi terus berkembang dan membentuk lanskap digital. Beberapa tren utama diperkirakan akan memengaruhi evolusi IoT di tahun-tahun mendatang (Román-Castro, López and Gritzalis, 2018).

Salah satu tren yang menonjol adalah proliferasi edge computing. Karena jumlah perangkat IoT tumbuh secara eksponensial, kebutuhan akan pemrosesan data real-time dan pengurangan latensi menjadi sangat penting. Komputasi tepi membawa pemrosesan data lebih dekat ke sumber data, memungkinkan waktu respons lebih cepat dan mengurangi transmisi data ke server cloud terpusat. Tren ini sangat relevan dalam aplikasi di mana pengambilan keputusan waktu nyata dan latensi rendah sangat penting, seperti kendaraan otonom dan otomasi industri.

Konvergensi 5G dan IoT adalah tren signifikan lainnya. Teknologi 5G memberikan kecepatan transfer data yang lebih tinggi, latensi yang lebih rendah, dan peningkatan kapasitas jaringan, yang penting untuk mendukung sejumlah besar perangkat dan aplikasi yang terhubung. 5G memungkinkan integrasi perangkat IoT tanpa hambatan dan memungkinkan kasus penggunaan baru yang menuntut komunikasi berkecepatan tinggi,

andal, dan latensi rendah, seperti augmented reality, operasi jarak jauh, dan penyebaran kota cerdas (Wakil *et al.*, 2022).



Gambar 2.1. Internet of Things
(Sumber : <https://binus.ac.id/>)

AI dan pembelajaran mesin siap untuk memainkan peran yang semakin penting dalam sistem IoT. Seiring bertambahnya volume data yang dihasilkan oleh perangkat IoT, kebutuhan akan analitik dan wawasan data tingkat lanjut menjadi lebih jelas. Algoritme yang didukung AI dapat menganalisis data dalam jumlah besar secara real-time, memungkinkan pemeliharaan prediktif, deteksi anomali, dan pengalaman pengguna yang dipersonalisasi. Aplikasi IoT berbasis AI akan menghasilkan sistem yang lebih otonom dan cerdas, meningkatkan efisiensi dan pengambilan keputusan di berbagai industri (Lalit *et al.*, 2022).

Sementara masa depan IoT menarik, ia juga menghadirkan tantangan signifikan yang harus diatasi agar teknologi dapat mencapai potensi penuhnya (Indrawan, no date).

Keamanan tetap menjadi perhatian utama dalam penerapan IoT. Seiring bertambahnya jumlah perangkat yang terhubung, demikian pula serangan yang muncul untuk potensi ancaman dunia maya. Mengamankan perangkat IoT dari serangan dunia maya dan memastikan privasi data merupakan tantangan penting. Banyak perangkat IoT tidak memiliki fitur keamanan bawaan, membuatnya rentan untuk dieksploitasi oleh peretas. Mengatasi celah keamanan ini memerlukan upaya bersama untuk menerapkan langkah-langkah keamanan yang kuat, seperti enkripsi, boot aman, dan pembaruan over-the-air, di seluruh ekosistem IoT (Atlam *et al.*, 2020).

Interoperabilitas adalah tantangan lain dalam lanskap IoT. Keragaman perangkat, protokol, dan platform IoT sering kali menyebabkan fragmentasi dan kurangnya komunikasi tanpa batas antara sistem yang berbeda. Pencapaian interoperabilitas sangat penting untuk memungkinkan komunikasi lintas platform dan pertukaran data, memungkinkan beragam perangkat IoT untuk bekerja bersama secara kohesif. Standardisasi di seluruh industri dan protokol terbuka akan sangat penting dalam mengatasi tantangan ini dan mendorong ekosistem IoT yang lebih terhubung dan dapat dioperasikan.

Skalabilitas menjadi perhatian karena penyebaran IoT tumbuh lebih besar dan lebih kompleks. Mendukung peningkatan jumlah perangkat yang terhubung dan mengelola pertumbuhan data yang eksponensial menimbulkan tantangan yang signifikan untuk infrastruktur IoT. Arsitektur yang dapat diskalakan, solusi berbasis cloud, dan edge computing adalah strategi utama untuk mengatasi tantangan ini dan memastikan ekosistem IoT tetap fleksibel dan dapat beradaptasi dengan permintaan yang berkembang (Román-Castro, López and Gritzalis, 2018).

Privasi data dan pertimbangan etis juga menjadi yang terdepan dalam aplikasi IoT. Dengan banyaknya data yang dikumpulkan dari perangkat IoT, kekhawatiran tentang kepemilikan data, persetujuan, dan potensi penyalahgunaan data

menjadi hal yang terpenting. Menetapkan pedoman dan peraturan yang jelas untuk melindungi privasi pengguna dan memastikan penggunaan data yang bertanggung jawab akan sangat penting dalam membangun kepercayaan dan mendorong adopsi teknologi IoT yang lebih luas.

Masa depan IoT ditandai dengan tren menarik yang berpotensi mengubah industri dan kehidupan kita sehari-hari. Komputasi tepi, integrasi 5G, dan aplikasi berbasis AI akan mendorong evolusi IoT. Namun, tantangan seperti keamanan, interoperabilitas, skalabilitas, dan privasi data harus diatasi untuk membuka potensi penuh IoT dan menciptakan masa depan yang terhubung dan berkelanjutan. Dengan mengatasi tantangan ini secara proaktif dan memanfaatkan teknologi baru, ekosistem IoT dapat terus berkembang, mendorong inovasi, dan membentuk dunia yang lebih terhubung dan cerdas (Al Aidhi *et al.*, 2023).

DAFTAR PUSTAKA

- Abdel-Basset, M. *et al.* 2019. 'Internet of things in smart education environment: Supportive framework in the decision-making process', *Concurrency and Computation: Practice and Experience*, 31(10), p. e4515.
- Ageed, Z.S. *et al.* 2021. 'Comprehensive survey of big data mining approaches in cloud systems', *Qubahan Academic Journal*, 1(2), pp. 29–38.
- Al Aidhi, A. *et al.* 2023. 'Peningkatan Daya Saing Ekonomi melalui peranan Inovasi', *Jurnal Multidisiplin West Science*, 2(02), pp. 118–134.
- Al-Qaseemi, S.A. *et al.* 2016. 'IoT architecture challenges and issues: Lack of standardization', in *2016 Future technologies conference (FTC)*. IEEE, pp. 731–738.
- Al-Sarawi, S. *et al.* 2017. 'Internet of Things (IoT) communication protocols', in *2017 8th International conference on information technology (ICIT)*. IEEE, pp. 685–690.
- An, J., Gui, X.-L. and He, X. 2012. 'Study on the architecture and key technologies for internet of things', *Advances in Biomedical Engineering*, 11, p. 329.
- Ardito, L. *et al.* 2019. 'A bibliometric analysis of research on Big Data analytics for business and management', *Management Decision*, 57(8), pp. 1993–2009.
- Atlam, H.F. *et al.* 2020. 'Security, cybercrime and digital forensics for IoT', *Principles of internet of things (IoT) ecosystem: Insight paradigm*, pp. 551–577.
- Baig, M.I., Shuib, L. and Yadegaridehkordi, E. 2019. 'Big data adoption: State of the art and research challenges', *Information Processing & Management*, 56(6), p. 102095.
- Bishop, M. 2004. *Introduction to computer security*. Addison-Wesley Professional.

- Cao, B. *et al.* 2019. 'When Internet of Things meets blockchain: Challenges in distributed consensus', *IEEE Network*, 33(6), pp. 133–139.
- Cheng, R. *et al.* 2022. 'Will metaverse be nextg internet? vision, hype, and reality', *IEEE Network*, 36(5), pp. 197–204.
- Choubey, D.K. *et al.* 2022. 'A review on IoT architectures, protocols, security, and applications', *Industrial Internet of Things*, pp. 225–242.
- Çorak, B.H. *et al.* 2018. 'Comparative analysis of IoT communication protocols', in *2018 International symposium on networks, computers and communications (ISNCC)*. IEEE, pp. 1–6.
- Davies, D.W. and Price, W.L. 1984. *Security for computer networks: an introduction to data security in teleprocessing and electronic funds transfer*. John Wiley & Sons, Inc.
- Davies, J. and Fortuna, C. 2020. *The Internet of Things: From Data to Insight*. John Wiley & Sons.
- Dizdarević, J. *et al.* 2019. 'A survey of communication protocols for internet of things and related challenges of fog and cloud computing integration', *ACM Computing Surveys (CSUR)*, 51(6), pp. 1–29.
- Dong, J.Q. and Yang, C.-H. 2020. 'Business value of big data analytics: A systems-theoretic approach and empirical test', *Information & Management*, 57(1), p. 103124.
- Dongsheng, Y. *et al.* 2019. 'Key technologies and application prospects of ubiquitous power internet of things', *Power generation technology*, 40(2), pp. 107–114.
- Ferraris, A. *et al.* 2019. 'Big data analytics capabilities and knowledge management: impact on firm performance', *Management Decision*, 57(8), pp. 1923–1936.
- Ganchev, I., Ji, Z. and O'Droma, M. 2014. 'A generic IoT architecture for smart cities'.
- Gerodimos, A. *et al.* 2023. 'IoT: Communication protocols and security threats', *Internet of Things and Cyber-Physical Systems* [Preprint].

- Gupta, B.B. and Quamara, M. 2020. 'An overview of Internet of Things (IoT): Architectural aspects, challenges, and protocols', *Concurrency and Computation: Practice and Experience*, 32(21), p. e4946.
- Indrawan, A.J. (no date) 'IoT dan Blockchain: Tinjauan Tantangan Solusi Keamanan dan Privasi'.
- Jabraeil Jamali, M.A. *et al.* 2020. 'IoT architecture', *Towards the Internet of Things: Architectures, Security, and Applications*, pp. 9–31.
- Khari, M. *et al.* 2016. 'Internet of Things: Proposed security aspects for digitizing the world', in *2016 3rd international conference on computing for sustainable global development (INDIACom)*. IEEE, pp. 2165–2170.
- Krčo, S., Pokrić, B. and Carrez, F. 2014. 'Designing IoT architecture (s): A European perspective', in *2014 IEEE world forum on internet of things (WF-IoT)*. IEEE, pp. 79–84.
- Kumar, G. *et al.* 2021. 'Internet-of-Forensic (IoF): A blockchain based digital forensics framework for IoT applications', *Future Generation Computer Systems*, 120, pp. 13–25.
- 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), pp. 1–21.
- Kyriakakis, E., Sparsø, J. and Schoeberl, M. 2019. 'Implementing time-triggered communication over a standard ethernet switch', in *Proceedings of the Workshop on Fog Computing and the IoT*, pp. 21–25.
- Lalit, M. *et al.* 2022. 'IoT networks: Security vulnerabilities of application layer protocols', in *2022 14th International Conference on Mathematics, Actuarial Science, Computer Science and Statistics (MACS)*. IEEE, pp. 1–5.
- Lavric, A. and Petrariu, A.I. 2018. 'LoRaWAN communication protocol: The new era of IoT', in *2018 International Conference on Development and Application Systems (DAS)*. IEEE, pp. 74–77.

- Liu, Y. and Zhou, G. 2012. 'Key technologies and applications of internet of things', in *2012 Fifth International Conference on Intelligent Computation Technology and Automation*. IEEE, pp. 197–200.
- Lloret, J. *et al.* 2016. 'An integrated IoT architecture for smart metering', *IEEE Communications Magazine*, 54(12), pp. 50–57.
- Ma, H.-D. 2011. 'Internet of things: Objectives and scientific challenges', *Journal of Computer science and Technology*, 26(6), pp. 919–924.
- Meutia, E.D. 2015. 'Internet of things–Keamanan dan Privasi', in *Seminar Nasional dan Expo Teknik Elektro*, pp. 85–89.
- Mikalef, P. *et al.* 2019. 'Big data and business analytics: A research agenda for realizing business value'.
- Moraes, T. *et al.* 2019. 'Performance comparison of IoT communication protocols', in *2019 IEEE International Conference on Systems, Man and Cybernetics (SMC)*. IEEE, pp. 3249–3254.
- Mughal, A.A. 2022. 'Well-Architected Wireless Network Security', *Journal of Humanities and Applied Science Research*, 5(1), pp. 32–42.
- Mulyana, E. *et al.* 2019. 'Analisis dan Perancangan Arsitektur Sistem Aplikasi Layanan Informasi Lokasi Berbasis IoT', in *Prosiding Seminar Nasional Teknik Elektro UIN Sunan Gunung Djati Bandung*, pp. 243–252.
- Ngiam, K.Y. and Khor, W. 2019. 'Big data and machine learning algorithms for health-care delivery', *The Lancet Oncology*, 20(5), pp. e262–e273.
- Novianto, E., Ujianto, E.H.H. and Rianto, R. 2023. 'KEAMANAN INFORMASI (INFORMATION SECURITY) PADA APLIKASI SISTEM INFORMASI MANAJEMEN SUMBER DAYA MANUSIA', *Rabit: Jurnal Teknologi dan Sistem Informasi Univrab*, 8(1), pp. 10–15.

- Oesterreich, T.D., Anton, E. and Teuteberg, F. 2022. 'What translates big data into business value? A meta-analysis of the impacts of business analytics on firm performance', *Information & Management*, 59(6), p. 103685.
- Pamarthi, S. and Narmadha, R. 2022. 'Literature review on network security in Wireless Mobile Ad-hoc Network for IoT applications: Network attacks and detection mechanisms', *International Journal of Intelligent Unmanned Systems*, 10(4), pp. 482–506.
- Rijal, S. *et al.* 2023. *Manajemen Sumber Daya Manusia*. Global Eksekutif Teknologi.
- Román-Castro, R., López, J. and Gritzalis, S. 2018. 'Evolution and trends in IoT security', *Computer*, 51(7), pp. 16–25.
- Rozi, F. 2020. 'Systematic Literature Review pada Analisis Prediktif dengan IoT: Tren Riset, Metode, dan Arsitektur', *Jurnal Sistem Cerdas*, 3(1), pp. 43–53.
- Rukmana, A.Y. 2023. 'BAB 3 TEKNOLOGI DIGITAL', *Digital Marketing Dan E-Commerce*, p. 27.
- Rukmana, A.Y. *et al.* 2023. *PENGANTAR SISTEM INFORMASI: Panduan Praktis Pengenalan Sistem Informasi & Penerapannya*. PT. Sonpedia Publishing Indonesia.
- Sadhu, P.K., Yanambaka, V.P. and Abdelgawad, A. 2022. 'Internet of Things: Security and Solutions Survey', *Sensors*, 22(19), p. 7433.
- Samaila, M.G. *et al.* 2017. 'Security challenges of the Internet of Things', *Beyond the internet of things: Everything interconnected*, pp. 53–82.
- Setiaji, G.I., Sofwan, A. and Sumardi, S. 2019. 'Perancangan Power Monitoring System Pada Panel Surya Sebagai Sumber Utama Pada Smart Open Parking Dalam Arsitektur Iot', *Transient: Jurnal Ilmiah Teknik Elektro*, 7(3), pp. 819–825.
- Setiawan, Z. *et al.* 2023. *Kewirausahaan Digital*. Global Eksekutif Teknologi.

- Shalaginov, A., Iqbal, A. and Olegård, J. 2020. 'Iot digital forensics readiness in the edge: A roadmap for acquiring digital evidences from intelligent smart applications', in *Edge Computing-EDGE 2020: 4th International Conference, Held as Part of the Services Conference Federation, SCF 2020, Honolulu, HI, USA, September 18-20, 2020, Proceedings 4*. Springer, pp. 1-17.
- Sharma, C. and Gondhi, N.K. 2018. 'Communication protocol stack for constrained IoT systems', in *2018 3rd International Conference On Internet of Things: Smart Innovation and Usages (IoT-SIU)*. IEEE, pp. 1-6.
- Song, T. *et al.* 2017. 'A privacy preserving communication protocol for IoT applications in smart homes', *IEEE Internet of Things Journal*, 4(6), pp. 1844-1852.
- Sun, Q., Liu, J. and Li, S. 2010. 'Internet of things: summarize on concepts, architecture and key technology problem', *Journal of Beijing University of Posts and Telecommunications*, 33(3), p. 1.
- Sunyaev, A. and Sunyaev, A. 2020. 'The internet of things', *Internet Computing: Principles of Distributed Systems and Emerging Internet-Based Technologies*, pp. 301-337.
- Sutaguna, I.N.T. *et al.* 2023. 'Training on Business Planning Using Business Canvas Models', *Cakrawala: Jurnal Pengabdian Masyarakat Global*, 2(3), pp. 34-43.
- Thangaramya, K. *et al.* 2019. 'Energy aware cluster and neuro-fuzzy based routing algorithm for wireless sensor networks in IoT', *Computer Networks*, 151, pp. 211-223.
- Tripathy, B.K. and Anuradha, J. 2017. *Internet of things (IoT): technologies, applications, challenges and solutions*. CRC press.
- Ukil, A., Sen, J. and Koilakonda, S. 2011. 'Embedded security for Internet of Things', in *2011 2nd National Conference on Emerging Trends and Applications in Computer Science*. IEEE, pp. 1-6.

- VARGA, M. and KUJUNDZIC, M. 2022. Innovative Technologies of Web Services and Security Protocols', *Co-Editors*, p. 35.
- Vitari, C. and Raguseo, E. 2020. 'Big data analytics business value and firm performance: linking with environmental context', *International Journal of Production Research*, 58(18), pp. 5456–5476.
- Wakil, A. *et al.* 2022. *Transformasi Digital Dalam Dunia Bisnis*. Global Eksekutif Teknologi.
- Wang, Y. *et al.* 2022. 'A survey on metaverse: Fundamentals, security, and privacy', *IEEE Communications Surveys & Tutorials* [Preprint].
- Wilianto, W. and Kurniawan, A. 2018. 'Sejarah, cara kerja dan manfaat internet of things', *Matrix: Jurnal Manajemen Teknologi Dan Informatika*, 8(2), pp. 36–41.
- Xiaohui, X. 2013. 'Study on security problems and key technologies of the internet of things', in *2013 International conference on computational and information sciences*. IEEE, pp. 407–410.
- Yathiraju, N. *et al.* 2022. 'Cybersecurity Capabilities in Developing Nations and Its Impact on Global Security: A Survey of Social Engineering Attacks and Steps for Mitigation of These Attacks', in *Cybersecurity Capabilities in Developing Nations and Its Impact on Global Security*. IGI global, pp. 110–132.
- Yue, Z. *et al.* 2015. 'Internet of things: Architecture, technology and key problems in implementation', in *2015 8th International Congress on Image and Signal Processing (CISP)*. IEEE, pp. 1298–1302.
- Zhong, C.-L., Zhu, Z. and Huang, R.-G. 2015. 'Study on the IOT architecture and gateway technology', in *2015 14th International Symposium on Distributed Computing and Applications for Business Engineering and Science (DCABES)*. IEEE, pp. 196–199.

BAB 3

INFRASTRUKTUR INTERNET OF THINGS

Oleh Irmawati

3.1 Pengenalan Infrastruktur Internet of Things

Infrastruktur *Internet of Things* (IoT) merupakan fondasi teknologi yang mendukung konektivitas dan interaksi antara berbagai perangkat fisik, kendaraan, sensor, dan perangkat lainnya melalui jaringan internet. Konsep utama di balik IoT adalah memungkinkan objek-objek ini untuk mengumpulkan, mengirim, dan menerima data secara otonom tanpa perlu intervensi manusia. Infrastruktur IoT mencakup berbagai elemen penting, termasuk perangkat IoT yang dilengkapi dengan sensor untuk mendeteksi lingkungan fisik, berbagai teknologi jaringan seperti WiFi, Bluetooth, dan *Low-Power Wide Area Network* (LPWAN) yang memungkinkan konektivitas, serta sistem komputasi baik di tepi (*edge computing*) maupun di cloud untuk memproses dan menganalisis data yang dihasilkan (Abdmeziem, Tandjaoui and Romdhani, 2016).

Keamanan merupakan komponen penting dalam infrastruktur IoT, mengingat tingginya risiko serangan siber pada perangkat yang terhubung ke internet. Penggunaan protokol keamanan, enkripsi data, dan sistem otentikasi diperlukan untuk melindungi data pribadi dan mencegah potensi ancaman keamanan. Selain itu, infrastruktur IoT juga harus mencakup sistem manajemen perangkat yang efisien untuk memantau, mengelola, dan memperbarui perangkat secara keseluruhan.

Infrastruktur IoT membuka berbagai peluang diberbagai sektor, termasuk industri, pertanian, kesehatan, transportasi, dan

lainnya. Dengan menghubungkan objek dan mengumpulkan data secara luas, infrastruktur IoT memungkinkan pengambilan keputusan yang lebih cerdas dan efisien, peningkatan produktivitas, dan pelayanan yang lebih baik kepada masyarakat. Namun, tantangan yang muncul termasuk skala dan kompleksitas infrastruktur, interoperabilitas perangkat dari berbagai vendor, dan tantangan privasi dan etika dalam pengelolaan data yang dikumpulkan.

Pengenalan infrastruktur IoT ini menandai era transformasi digital yang semakin pesat, dimana konektivitas dan integrasi perangkat semakin memainkan peran kunci dalam cara kita hidup, bekerja, dan berinteraksi dengan lingkungan sekitar. Pengembangan infrastruktur IoT yang kuat dan aman akan menjadi pendorong utama inovasi dan perubahan positif dalam berbagai aspek kehidupan dimasa depan.

3.2 Komponen Infrastruktur IoT

Komponen infrastruktur IoT mencakup berbagai elemen yang bekerja bersama untuk menghubungkan, mengumpulkan data, dan mengelola perangkat IoT (Kranz, 2016). Salah satu komponen utama dalam infrastruktur IoT adalah perangkat IoT itu sendiri. Perangkat IoT berperan sebagai sensor, aktuator, atau perangkat pintar lainnya yang memungkinkan pengumpulan data dari lingkungannya atau mengambil tindakan berdasarkan data yang dikumpulkan. Contoh perangkat IoT termasuk sensor suhu, perangkat pintar di rumah, kendaraan terhubung, dan banyak lagi. Keberadaan perangkat IoT yang andal dan canggih penting untuk menciptakan lingkungan yang terkoneksi dengan baik (Bhattacharjee, 2018).

Selain perangkat IoT, jaringan komunikasi adalah elemen penting lainnya dalam infrastruktur IoT. Jaringan komunikasi memungkinkan perangkat IoT untuk berkomunikasi dengan infrastruktur lainnya, seperti platform cloud atau sistem analitik.

Jenis jaringan komunikasi yang digunakan dapat bervariasi tergantung pada jarak dan kebutuhan daya baterai perangkat IoT. Beberapa teknologi nirkabel yang umum digunakan dalam IoT termasuk Wi-Fi, Bluetooth, Zigbee, dan jaringan seluler seperti 4G/5G. Memilih jaringan komunikasi yang tepat adalah kunci untuk memastikan konektivitas yang andal antara perangkat IoT dan infrastruktur pusat.

Selanjutnya, gateway berfungsi sebagai penghubung antara perangkat IoT dan platform cloud atau sistem analitik. Gateway membantu menerjemahkan data dari berbagai protokol yang digunakan oleh perangkat IoT sehingga data dapat diolah dan dimengerti oleh sistem pusat. Selain itu, gateway juga bertindak sebagai filter data dan membantu dalam pengelolaan koneksi untuk banyak perangkat IoT. Integrasi gateway yang efisien sangat penting dalam mengelola lalu lintas data IoT yang besar dari berbagai perangkat.

Platform cloud adalah komponen infrastruktur lainnya yang berperan penting dalam pengelolaan dan analisis data dari perangkat IoT. Data yang dikumpulkan dari perangkat IoT dikirim ke platform cloud untuk disimpan dan dianalisis lebih lanjut. Cloud platform menyediakan kapasitas penyimpanan yang besar dan kemampuan analisis data real-time untuk menghasilkan wawasan yang berharga. Platform ini juga menyediakan antarmuka bagi pengguna atau pengelola untuk mengakses data dan mengelola perangkat IoT dari jarak jauh.

Terakhir, aspek keamanan dan privasi adalah hal yang tak terpisahkan dalam infrastruktur IoT. Karena perangkat IoT mengumpulkan dan mentransmisikan data sensitif, perlindungan keamanan yang kuat sangat diperlukan. Protokol enkripsi, otentikasi yang aman, dan kebijakan keamanan yang ketat harus diimplementasikan untuk melindungi data dari akses yang tidak sah atau serangan. Selain itu, perangkat IoT itu sendiri juga harus memiliki lapisan keamanan yang memadai untuk melindungi dari potensi eksploitasi keamanan.

3.2.1 Jaringan dan Protokol Komunikasi

Jaringan komunikasi adalah sistem yang memungkinkan perangkat elektronik, seperti komputer, telepon, tablet, dan perangkat lainnya, untuk berkomunikasi dan bertukar data satu sama lain. Tujuan utama dari jaringan adalah memungkinkan perangkat untuk berbagi informasi dan sumber daya, seperti data, file, printer, koneksi internet, dan perangkat lainnya.

Jaringan komunikasi menggunakan protokol komunikasi untuk mengatur bagaimana data dikirim, diterima, dan diproses antara perangkat yang terhubung (Kurose and Ross, 2010). Protokol komunikasi adalah aturan dan standar yang diikuti oleh perangkat untuk berkomunikasi secara efisien. Protokol ini menentukan cara perangkat mengidentifikasi satu sama lain di jaringan, cara menginisiasi dan mengakhiri sesi komunikasi, serta cara mengatur dan memvalidasi data yang ditransfer.

Contoh kasus jaringan dan protokol komunikasi adalah internet, yang merupakan jaringan global yang menghubungkan miliaran perangkat di seluruh dunia. Protokol yang digunakan di internet termasuk TCP/IP (*Transmission Control Protocol/Internet Protocol*). Protokol TCP bertanggung jawab untuk memastikan data terkirim dengan aman dan benar dengan memeriksa kehilangan paket dan mengaturnya ulang jika diperlukan. Sementara itu, protokol IP bertanggung jawab untuk mengarahkan paket data ke tujuan yang benar melalui alamat IP.

Contoh kasus dan studi literatur di atas memberikan gambaran tentang pentingnya jaringan dan protokol komunikasi dalam menghubungkan perangkat dan memfasilitasi pertukaran informasi di dunia digital yang semakin terkoneksi. Studi literatur tersebut dapat membantu dalam memahami dasar-dasar jaringan dan protokol serta berbagai aspek yang lebih canggih, seperti keamanan jaringan dan teknologi nirkabel.

3.2.2 Cloud Computing dan Edge Computing

Cloud Computing adalah paradigma komputasi yang memungkinkan akses, penyimpanan, dan manajemen sumber daya komputasi melalui internet. Pengguna dapat mengakses dan menggunakan infrastruktur IT, seperti server, penyimpanan data, dan perangkat lunak, tanpa harus memiliki perangkat keras fisik. Layanan cloud disajikan dalam berbagai model, termasuk *Software as a Service* (SaaS), *Platform as a Service* (PaaS), dan *Infrastructure as a Service* (IaaS) (Erl, Puttini and Mahmood, 2013). SaaS menyediakan aplikasi perangkat lunak melalui internet, PaaS menyediakan platform untuk mengembangkan aplikasi, dan IaaS menyediakan sumber daya infrastruktur. Cloud Computing memberikan keuntungan seperti skalabilitas, elastisitas, dan efisiensi, karena pengguna dapat menyesuaikan sumber daya sesuai permintaan tanpa harus berinvestasi dalam infrastruktur yang mahal.

Edge Computing merupakan paradigma komputasi yang menempatkan proses data dan komputasi lebih dekat dengan sumber data dan perangkat akhir, daripada diproses di pusat data yang jauh. Dalam Edge Computing, pengolahan data terjadi ditepi jaringan, dekat dengan sumber data atau perangkat, yang membantu mengurangi latensi dan mempercepat waktu respon (Cao, Zhang and Shi, 2018). Pendekatan ini sangat relevan untuk aplikasi yang memerlukan respon waktu nyata atau sangat rendah, seperti *Internet of Things* (IoT), mobil otonom, dan sistem yang memerlukan analisis data real-time. *Edge Computing* memberikan keuntungan dalam mengatasi kendala bandwidth dan mengurangi beban pada jaringan pusat data.

Studi kasus yang melibatkan *Cloud Computing* adalah perusahaan e-commerce terkemuka, seperti Amazon. Amazon menggunakan layanan cloud mereka sendiri, yaitu *Amazon Web Services* (AWS), untuk menyediakan platform e-commerce mereka. Dengan menggunakan model IaaS dari AWS, Amazon dapat menyewa sumber daya komputasi dan penyimpanan sesuai

permintaan dan kebutuhan mereka. Dengan demikian, Amazon dapat mengelola arus lalu lintas yang fluktuatif dan memastikan situs web mereka tetap berkinerja tinggi selama periode promosi atau penjualan besar-besaran, seperti Hari Belanja Online (*Black Friday*). Layanan cloud memungkinkan Amazon untuk menawarkan layanan yang andal, skalabel, dan efisien bagi pelanggan mereka tanpa harus mengelola infrastruktur fisik secara langsung.

Studi kasus untuk Edge Computing, kita dapat melihat penerapan teknologi kendaraan otonom. Kendaraan otonom memerlukan analisis data yang cepat dan respon waktu yang sangat rendah untuk beroperasi dengan aman dan efisien. Dalam sistem kendaraan otonom, sensor di mobil menghasilkan sejumlah besar data yang harus diproses secara instan. Menggunakan Edge Computing, sebagian besar analisis data dan pengambilan keputusan dapat dilakukan di dalam mobil itu sendiri atau di sistem komputasi yang terdekat, mengurangi ketergantungan pada cloud dan mengurangi latensi. Hal ini memungkinkan kendaraan otonom untuk merespons situasi dengan lebih cepat dan mengoptimalkan kinerjanya, meningkatkan keamanan dan kenyamanan bagi pengguna jalan.

Kedua studi kasus tersebut menunjukkan bagaimana *Cloud Computing* dan *Edge Computing* memberikan solusi untuk berbagai tantangan dan kasus penggunaan di dunia nyata, membantu organisasi dan industri mencapai efisiensi, skalabilitas, dan kinerja yang lebih baik.

3.3 Keamanan dalam Infrastruktur IoT

Keamanan dalam Infrastruktur *Internet of Things* (IoT) merupakan salah satu aspek yang sangat penting dalam era konektivitas dan digitalisasi saat ini. Infrastruktur IoT melibatkan jaringan perangkat dan sistem yang berkomunikasi dan berinteraksi satu sama lain untuk mengumpulkan,

mentransmisikan, dan menganalisis data dari berbagai sensor dan perangkat cerdas. Namun, semakin banyaknya perangkat terhubung dan kompleksitas infrastruktur IoT membawa potensi risiko keamanan yang serius.

Salah satu tantangan utama dalam keamanan IoT adalah kerentanannya terhadap serangan siber. Perangkat IoT yang kurang aman dapat menjadi pintu masuk bagi peretas untuk mengakses data sensitif, mencuri informasi pribadi, atau menyebabkan gangguan dan kerusakan. Serangan DDoS (Distributed Denial of Service) juga menjadi ancaman, di mana perangkat IoT yang terinfeksi dapat digunakan untuk menyerang sistem lain dengan membanjiri lalu lintas jaringan (Alferidah and Jhanjhi, 2020).

Selain itu, keamanan data juga menjadi perhatian utama. Data yang dikumpulkan dan ditransmisikan oleh perangkat IoT seringkali mengandung informasi pribadi atau rahasia yang harus dilindungi dari akses yang tidak sah. Jika data ini jatuh ke tangan yang salah, maka privasi pengguna dapat terancam. Tantangan lainnya adalah kerentanannya pada perangkat IoT itu sendiri. Beberapa perangkat mungkin memiliki kelemahan dalam sistem keamanan mereka, dan pembaruan perangkat lunak yang kurang teratur dapat meninggalkan celah yang dapat disusupi oleh penyerang.

Untuk mengatasi tantangan keamanan dalam infrastruktur IoT, perlu diambil langkah-langkah proaktif. Pengamanan perangkat IoT harus menjadi prioritas selama proses desain dan pengembangan. Perusahaan harus menggunakan enkripsi data untuk melindungi data yang dikumpulkan dan ditransmisikan, serta menerapkan metode otentikasi yang kuat untuk memastikan bahwa hanya perangkat yang sah yang diizinkan untuk berkomunikasi dengan infrastruktur IoT. Selain itu, pemantauan dan analisis keamanan secara *real-time* diperlukan untuk mendeteksi dan mengatasi ancaman dengan cepat.

Standar keamanan yang konsisten juga harus diterapkan untuk memastikan bahwa semua perangkat IoT mematuhi praktik keamanan terbaik. Selain itu, edukasi dan kesadaran tentang keamanan IoT harus ditingkatkan baik di kalangan pengguna maupun produsen perangkat.

Dengan mengambil langkah-langkah ini, infrastruktur IoT dapat menjadi lebih aman dan dapat diandalkan, sehingga potensi inovasi dan manfaat dari IoT dapat diwujudkan tanpa mengorbankan keamanan dan privasi. Keamanan dalam infrastruktur IoT harus menjadi prioritas yang tidak boleh diabaikan bagi masyarakat dan industri di era konektivitas dan teknologi yang terus berkembang.

3.3.1 Tantangan Keamanan dan Privasi

Tantangan keamanan dan privasi adalah dua isu krusial yang terus berkembang di era digital saat ini. Dalam era di mana teknologi informasi mengalami kemajuan pesat, kita dihadapkan pada risiko dan ancaman yang semakin kompleks terkait keamanan data dan informasi pribadi. Tantangan keamanan meliputi serangan siber seperti peretasan, malware, dan phishing yang dapat mengakibatkan pencurian data sensitif, kerugian finansial, dan bahkan potensi bocornya informasi rahasia negara atau perusahaan.

Di sisi lain, tantangan privasi berkaitan dengan bagaimana data pribadi kita dikumpulkan, digunakan, dan disebarkan oleh berbagai entitas, termasuk perusahaan dan pemerintah. Dengan makin meluasnya penggunaan teknologi dan internet, informasi pribadi kita menjadi lebih mudah diakses dan diekspos. Kekhawatiran tentang privasi mencakup pelacakan online, profilisasi pengguna, dan penggunaan data tanpa izin yang dapat menimbulkan masalah etika dan pelanggaran hak asasi manusia.

Penyelesaian tantangan keamanan dan privasi membutuhkan kerjasama antara pemerintah, perusahaan, dan masyarakat. Perlindungan data yang kuat dan kebijakan privasi yang ketat harus diterapkan untuk memastikan informasi sensitif

tidak jatuh ke tangan yang salah. Selain itu, kesadaran masyarakat tentang ancaman keamanan dan hak privasi mereka perlu ditingkatkan agar mereka dapat mengambil langkah-langkah pencegahan yang tepat, seperti menghindari praktik-praktik yang berisiko atau menggunakan alat keamanan digital yang efektif. Dengan menghadapi tantangan ini dengan sungguh-sungguh, kita dapat menciptakan lingkungan digital yang lebih aman dan menghormati privasi individual di dunia yang semakin terhubung.

Tantangan keamanan terkait dengan perlindungan terhadap data dan sistem informasi dari akses yang tidak sah, peretasan, dan serangan siber lainnya. Beberapa tantangan keamanan meliputi (Elmaghraby and Losavio, 2014):

- a. Peretasan: Upaya pihak luar untuk mengakses informasi atau mengendalikan sistem yang tidak sah. Serangan siber dapat menyebabkan pencurian data sensitif, kerusakan infrastruktur, atau penyebaran malware.
- b. Keamanan Perangkat Mobile: Dengan semakin banyaknya pengguna perangkat mobile seperti smartphone dan tablet, keamanan perangkat ini menjadi penting. Ancaman termasuk aplikasi berbahaya, peretasan perangkat, dan serangan melalui jaringan nirkabel.
- c. *Internet of Things* (IoT): Pertumbuhan IoT membawa tantangan keamanan baru karena banyaknya perangkat terhubung yang mungkin rentan terhadap serangan dan dapat menyebabkan risiko privasi.
- d. Keamanan Cloud: Layanan cloud populer untuk menyimpan dan mengakses data, tetapi keamanan di cloud merupakan isu yang kompleks karena banyaknya data yang disimpan dan diakses oleh pihak ketiga.

Studi Kasus: Serangan WannaCry pada tahun 2017 adalah contoh serangan ransomware yang menyerang ribuan organisasi di seluruh dunia, termasuk layanan kesehatan dan sektor publik, menyebabkan kerugian besar.

3.4 Pengelolaan Perangkat IoT

Pengelolaan Perangkat IoT merupakan proses untuk merencanakan, mengimplementasikan, dan memantau perangkat yang terhubung ke Internet untuk mengumpulkan dan bertukar data secara nirkabel. Pengelolaan ini bertujuan untuk memastikan bahwa perangkat IoT beroperasi dengan efisien, aman, dan andal selama siklus hidupnya. Pengelolaan Perangkat IoT mencakup beberapa aspek penting berikut (Umar *et al.*, 2018):

1. Registrasi dan Otentikasi: Setiap perangkat IoT yang ingin terhubung ke jaringan harus terdaftar secara unik dan diotentikasi untuk mencegah akses yang tidak sah. Ini melibatkan penggunaan sertifikat, token, atau mekanisme otentikasi lainnya.
2. Provisioning: Langkah pertama dalam pengelolaan perangkat IoT adalah memastikan bahwa perangkat diberi konfigurasi dan firmware yang tepat sebelum digunakan. Proses ini melibatkan penyiapan parameter jaringan, kredensial, dan perangkat lunak untuk memungkinkan koneksi yang aman dan lancar.
3. Pemantauan dan Pengumpulan Data: Pengelolaan IoT melibatkan pemantauan status perangkat secara terus-menerus dan mengumpulkan data dari perangkat untuk analisis dan pengambilan keputusan. Data ini dapat digunakan untuk mendeteksi masalah, mengoptimalkan kinerja, dan meningkatkan pengalaman pengguna.
4. Pembaruan Perangkat Lunak: Keamanan dan kinerja perangkat IoT dapat meningkat melalui pembaruan perangkat lunak secara teratur. Pengelolaan perangkat IoT mencakup mekanisme yang memungkinkan pembaruan perangkat lunak yang mudah dan aman diimplementasikan pada perangkat.
5. Manajemen Energi: Perangkat IoT sering kali bekerja dengan daya baterai atau sumber daya terbatas lainnya.

Oleh karena itu, pengelolaan perangkat IoT harus memperhatikan penggunaan energi dan mengoptimalkan konsumsi daya agar masa pakai baterai lebih lama.

6. Keamanan dan Privasi: Pengelolaan perangkat IoT harus memprioritaskan keamanan dan privasi data. Ini melibatkan penggunaan enkripsi data, mengamankan akses ke perangkat, dan menerapkan protokol keamanan yang tepat untuk melindungi data dan sistem dari ancaman keamanan.
7. Manajemen Kapasitas: Ketika jumlah perangkat IoT terus bertambah, pengelolaan perangkat harus dapat memastikan infrastruktur jaringan dan cloud yang memadai untuk menangani beban yang semakin besar.
8. Pemantauan Kesehatan Perangkat: Pengelolaan perangkat IoT mencakup pemantauan kesehatan perangkat secara berkala untuk mendeteksi perangkat yang bermasalah atau berpotensi rusak. Ini memungkinkan tindakan pencegahan atau perbaikan yang cepat sebelum masalah menjadi lebih besar.
9. Manajemen Siklus Hidup: Pengelolaan perangkat IoT juga mencakup perencanaan untuk tahap akhir dari siklus hidup perangkat, termasuk daur ulang atau penghapusan data secara aman setelah penggunaan selesai.
10. Interoperabilitas: Perangkat IoT sering berasal dari berbagai produsen dan menggunakan berbagai protokol komunikasi. Pengelolaan perangkat IoT harus mencakup standarisasi dan interoperabilitas untuk memastikan bahwa perangkat dapat berkomunikasi dengan baik satu sama lain dan dengan sistem lain dalam ekosistem IoT.

Pengelolaan Perangkat IoT yang efektif dan komprehensif menjadi kunci untuk memastikan kesuksesan implementasi dan adopsi IoT secara luas dalam berbagai bidang, termasuk rumah pintar, industri, kesehatan, transportasi, dan lainnya.

3.5 Analisis Data IoT

Analisis Data IoT merupakan proses kritis dalam memahami dan menggali nilai dari data yang dihasilkan oleh berbagai perangkat terhubung dalam ekosistem IoT. Dalam era dimana perangkat-perangkat pintar semakin meluas, data yang dihasilkan oleh sensor, perangkat cerdas, dan objek terhubung lainnya menjadi semakin besar dan beragam. Analisis Data IoT bertujuan untuk menyaring, mengolah, dan menginterpretasi data tersebut guna mengidentifikasi pola, tren, serta mendapatkan wawasan yang bernilai bagi pengambilan keputusan dan peningkatan efisiensi. Teknik analisis data seperti *machine learning* dan algoritma kecerdasan buatan sering digunakan untuk menghadapi volume besar dan kerumitan data IoT, membantu mengidentifikasi informasi yang relevan dan memberikan wawasan yang mendalam (Perros, 2021).

Proses Analisis Data IoT terdiri dari beberapa tahap. Tahap pertama adalah pengumpulan data, di mana data diambil dari berbagai perangkat IoT dan disimpan dalam sistem penyimpanan yang sesuai. Selanjutnya, data tersebut harus diolah dan dibersihkan untuk menghilangkan data yang tidak valid, nilai yang hilang, atau outlier yang dapat mempengaruhi hasil analisis. Setelah itu, data disusun dan dipersiapkan untuk proses analisis, dimana berbagai metode seperti analisis statistik, prediksi, dan klasifikasi digunakan untuk mengungkap pola dan tren yang mendasari data IoT. Terakhir, hasil analisis tersebut diinterpretasikan dan divisualisasikan untuk mempermudah pemahaman dan pengambilan keputusan yang tepat.

Analisis Data IoT memiliki potensi besar untuk mendukung berbagai sektor dan industri. Dalam sektor kesehatan, data IoT dapat digunakan untuk mengumpulkan informasi tentang kesehatan pasien secara real-time dan memberikan peringatan dini tentang kondisi kesehatan yang memerlukan perhatian. Di sektor industri, analisis data IoT membantu memonitor kondisi peralatan

dan performa produksi, sehingga memungkinkan perusahaan untuk meningkatkan efisiensi operasional dan mencegah kegagalan peralatan. Selain itu, dibidang transportasi, data IoT dapat digunakan untuk memperbaiki rute dan mengoptimalkan logistik, mengurangi waktu perjalanan, dan mengurangi biaya operasional secara keseluruhan. Dengan menerapkan analisis data IoT secara cerdas, berbagai sektor dapat mengambil keuntungan penuh dari potensi revolusioner yang ditawarkan oleh teknologi IoT untuk mencapai tujuan yang lebih baik dan berkelanjutan.

3.5.1 Analisis Data dalam Infrastruktur IoT

Analisis data dalam infrastruktur IoT adalah proses yang melibatkan pengumpulan, penyimpanan, pengolahan, dan analisis data yang dihasilkan oleh perangkat IoT. Diawali dengan pengumpulan data dari berbagai perangkat terhubung seperti sensor, perangkat pintar, atau perangkat IoT lainnya yang menghasilkan data beragam, seperti informasi cuaca, tekanan, suhu, kelembaban, gerakan, dan banyak lagi, sesuai dengan tujuan dan jenis perangkat tersebut (Geng, 2017). Data yang telah dikumpulkan kemudian disimpan secara aman dalam sistem yang dapat diakses, bisa berupa penyimpanan lokal di perangkat itu sendiri atau di server terpusat, cloud, atau gabungan dari keduanya.

Selanjutnya, data diolah untuk membersihkan, normalisasi, agregasi, dan transformasi guna mengubahnya menjadi format yang lebih berguna untuk analisis. Setelah data diproses, tahap analisis data menjadi pusat perhatian dalam infrastruktur IoT. Proses analisis ini menggunakan teknik seperti analisis statistik, pembelajaran mesin, pembelajaran mendalam, dan kecerdasan buatan untuk mengidentifikasi pola, tren, anomali, dan informasi berharga lainnya dari data yang dikumpulkan. Hasil analisis ini berguna untuk mendukung pengambilan keputusan dan tindakan yang tepat, seperti merespons kondisi tertentu yang diindikasikan oleh data, memperbaiki kinerja sistem, mengoptimalkan operasi, dan memperbarui proses.

Contoh kasus penggunaan infrastruktur IoT dalam analisis data dapat dilakukan dalam berbagai bidang, salah satunya adalah memonitor kualitas udara di suatu kota. Dalam contoh ini, banyak sensor dipasang di berbagai titik di seluruh kota untuk mengukur tingkat polutan seperti PM2.5, NO2, SO2, dan CO. Data dari sensor-sensor ini dikumpulkan dan dianalisis untuk mengidentifikasi pola dan tren kualitas udara selama periode waktu tertentu. Berdasarkan hasil analisis data, kebijakan dapat dirumuskan untuk mengurangi polusi dan meningkatkan kualitas udara di kota tersebut.

Dengan analisis data dalam infrastruktur IoT, organisasi dan masyarakat dapat memanfaatkan informasi berharga dari data yang dihasilkan oleh perangkat IoT untuk meningkatkan efisiensi, mengoptimalkan operasi, dan mengambil keputusan yang lebih cerdas dalam berbagai bidang kehidupan sehari-hari.

3.6 Integrasi dan Interoperabilitas

Integrasi dan interoperabilitas memiliki peran sentral dalam membangun dan mengelola infrastruktur IoT, yang semakin berkembang dalam era terhubung saat ini. Integrasi dalam konteks IoT melibatkan penyatuan berbagai perangkat, platform, dan sistem yang beragam menjadi ekosistem yang terpadu. Hal ini memungkinkan data dari berbagai sumber mengalir dengan lancar, memperkuat efisiensi dan kerjasama antara komponen yang berbeda. Integrasi yang baik memfasilitasi optimisasi operasional, meningkatkan pemahaman melalui analisis data yang lebih mendalam, dan merangsang inovasi dengan memadukan berbagai teknologi.

Interoperabilitas adalah kunci untuk mengatasi hambatan komunikasi antara perangkat dan sistem yang berasal dari produsen yang berbeda atau menggunakan protokol yang beragam. Melalui penerapan standar komunikasi yang seragam, interoperabilitas memungkinkan perangkat IoT untuk berbicara

satu sama lain tanpa masalah, membuka pintu bagi kolaborasi dan pertukaran data yang lebih efektif. Dengan interoperabilitas yang baik, organisasi dengan mudah mengintegrasikan perangkat baru ke dalam lingkungan yang ada, mengurangi biaya pengembangan, dan merangsang pertumbuhan ekosistem IoT secara lebih dinamis.

Hasil akhir dari integrasi dan interoperabilitas yang sukses adalah infrastruktur IoT yang kokoh, responsif, dan mampu memberikan nilai tambah yang signifikan. Data yang dapat diakses dan dibagi dengan mudah memungkinkan pengambilan keputusan yang lebih baik, serta pengembangan solusi yang lebih cerdas dan adaptif. Dalam lingkungan bisnis yang cepat berubah, integrasi dan interoperabilitas yang baik dalam infrastruktur IoT membantu organisasi untuk tetap kompetitif dan siap menghadapi tantangan masa depan dengan cara yang lebih inovatif dan efisien (Perera *et al.*, 2014).

Manfaat Integrasi dalam Infrastruktur IoT:

1. Pengambilan Keputusan Menjadi Lebih Baik: Integrasi memungkinkan akses ke data dari berbagai sumber yang berbeda, memungkinkan pengambilan keputusan yang lebih informasional dan akurat.
2. Optimalisasi Operasional: Data yang terintegrasi memungkinkan proses bisnis dioptimalkan, mengurangi biaya dan waktu yang diperlukan.
3. Peningkatan Efisiensi: Integrasi memungkinkan aliran informasi yang lebih mulus dan kolaborasi antara perangkat, yang dapat meningkatkan efisiensi keseluruhan.
4. Kemampuan Analitik yang Lebih Baik: Data yang terintegrasi dapat digunakan untuk analisis yang lebih mendalam dan insight yang lebih baik.
5. Inovasi: Integrasi memungkinkan pengembangan solusi baru dan inovatif dengan memanfaatkan keahlian dari berbagai domain.

Manfaat Interoperabilitas dalam Infrastruktur IoT:

1. Kemudahan Integrasi: Interoperabilitas mempermudah integrasi perangkat baru ke dalam infrastruktur yang ada.
2. Pengurangan Biaya: Standardisasi dan interoperabilitas dapat mengurangi biaya pengembangan dan integrasi.
3. Peningkatan Fleksibilitas: Kemampuan perangkat untuk berinteraksi secara bebas meningkatkan fleksibilitas dan adaptabilitas infrastruktur.
4. Skalabilitas: Interoperabilitas memungkinkan pertumbuhan ekosistem IoT tanpa mengalami kesulitan komunikasi.

Contoh Implementasi:

Misalnya, dalam lingkungan pintu gerbang otomatis yang terhubung dengan jaringan IoT, integrasi memungkinkan pintu gerbang untuk berkomunikasi dengan sensor penginderaan lalu lintas, kamera pengawas, dan sistem manajemen lalu lintas. Interoperabilitas memastikan bahwa semua komponen tersebut dapat bekerja bersama, berbagi data tentang lalu lintas, dan mengambil tindakan seperti membuka atau menutup pintu gerbang sesuai dengan kondisi lalu lintas.

Integrasi dan interoperabilitas adalah elemen kunci dalam membangun dan mengelola infrastruktur IoT yang sukses. Keduanya membantu mengoptimalkan penggunaan data, meningkatkan efisiensi operasional, dan mendorong inovasi melalui kolaborasi dan keterhubungan yang lebih baik antara berbagai perangkat dan sistem.

3.6.1 Integrasi Infrastruktur IoT

Integrasi infrastruktur IoT dengan sistem yang ada merujuk pada proses menggabungkan teknologi IoT ke dalam sistem yang sudah ada dalam suatu organisasi atau lingkungan. Tujuannya adalah untuk memperluas kemampuan sistem yang ada dengan memanfaatkan data dan fungsionalitas yang dihasilkan oleh perangkat-perangkat IoT. Integrasi ini dapat memberikan manfaat

yang signifikan dalam hal efisiensi, pengambilan keputusan yang lebih baik, dan peningkatan kinerja secara keseluruhan. Berikut adalah cara integrasi infrastruktur IoT dengan sistem yang ada dapat dilakukan (Kranz, 2016):

1. Identifikasi Kebutuhan dan Tujuan
Pertama perlu diidentifikasi tujuan dari integrasi. Apakah kita ingin meningkatkan pemantauan, pengumpulan data, atau efisiensi operasional? Menentukan tujuan ini akan membantu kita dalam merancang strategi integrasi yang sesuai.
2. Pemilihan Perangkat IoT yang Sesuai
Pilih perangkat IoT yang sesuai dengan tujuan dan kebutuhan integrasi. Pastikan perangkat tersebut memiliki kemampuan kompatibilitas dengan sistem yang ada.
3. Konektivitas
Integrasi memerlukan koneksi antara perangkat IoT dan sistem yang ada. Pastikan perangkat memiliki kemampuan konektivitas yang sesuai dengan infrastruktur jaringan yang sudah ada.
4. Pengumpulan Data
Konfigurasi perangkat IoT untuk mengumpulkan data yang relevan. Data ini dapat mencakup informasi lingkungan, kinerja perangkat, atau parameter lain yang dapat memberikan wawasan penting.
5. Pemrosesan Data
Data yang dikumpulkan oleh perangkat IoT dapat diproses secara lokal di perangkat atau dikirim ke platform cloud untuk analisis lebih lanjut. Pemrosesan data ini dapat menghasilkan wawasan yang lebih mendalam.
6. Integrasi dengan Sistem yang Ada
Integrasi infrastruktur IoT memerlukan penggabungan data dan fungsionalitas perangkat IoT dengan sistem yang ada. Ini mungkin melibatkan pengembangan antarmuka atau integrasi langsung dengan sistem yang ada.

7. Analisis dan Pengambilan Keputusan

Data yang dikumpulkan dan diolah oleh perangkat IoT dapat digunakan untuk analisis yang lebih baik dan pengambilan keputusan yang lebih cerdas. Informasi ini dapat membantu meningkatkan efisiensi operasional atau mengidentifikasi peluang baru.

8. Aksi dan Respons Otomatis

Salah satu aspek kuat dari integrasi infrastruktur IoT adalah kemampuan untuk mengambil tindakan otomatis berdasarkan data yang diterima. Misalnya, sistem dapat mengirim peringatan atau memicu tindakan tertentu ketika kondisi tertentu terpenuhi.

9. Keamanan dan Privasi

Pastikan integrasi ini memperhatikan keamanan dan privasi data yang dikumpulkan oleh perangkat IoT. Data sensitif harus dilindungi dengan baik.

10. Pengembangan Lanjutan dan Pemeliharaan

Setelah integrasi berhasil diimplementasikan, pastikan untuk terus melakukan pemeliharaan, pemantauan, dan pengembangan lanjutan untuk memastikan bahwa sistem berjalan dengan baik dan sesuai dengan tujuan awal.

Integrasi infrastruktur IoT dengan sistem yang ada dapat memberikan manfaat signifikan dalam hal efisiensi, inovasi, dan pengambilan keputusan yang lebih baik. Namun, penting untuk merancang dan mengimplementasikan integrasi ini dengan hati-hati agar menghindari gangguan atau kerusakan pada sistem yang sudah ada.

3.7 Skalabilitas dan Fleksibilitas

Skalabilitas dan fleksibilitas merupakan dua konsep utama dalam desain dan pengelolaan infrastruktur IoT. Kedua konsep ini sangat penting untuk memastikan bahwa lingkungan IoT dapat

tumbuh dan berubah sesuai dengan kebutuhan yang terus berkembang. Mari kita jelaskan lebih detail tentang kedua konsep tersebut:

Skalabilitas mengacu pada kemampuan sistem untuk menangani peningkatan jumlah perangkat terhubung, volume data, dan permintaan layanan tanpa mengalami degradasi kinerja atau penurunan kualitas layanan (Li, Da Xu and Zhao, 2018). Dalam konteks infrastruktur IoT, skalabilitas berarti bahwa platform atau jaringan IoT harus mampu menangani pertumbuhan yang cepat dalam jumlah perangkat yang terhubung. Mencakup kemampuan untuk mengelola lebih banyak data yang dihasilkan oleh perangkat, menjaga ketersediaan layanan yang tinggi, dan menjaga latensi yang rendah.

Contoh Skalabilitas dalam Infrastruktur IoT:

Misalkan sebuah sistem pemantauan kesehatan menggunakan sensor-sensor IoT untuk mengumpulkan data dari pasien. Dengan skalabilitas yang baik, sistem ini dapat dengan mudah menambahkan lebih banyak pasien dan sensor tanpa mengganggu operasional keseluruhan atau mengurangi waktu respons.

Fleksibilitas merujuk pada kemampuan infrastruktur IoT untuk beradaptasi dengan perubahan kebutuhan atau kondisi tanpa memerlukan perubahan besar dalam desain atau arsitektur (Bassi *et al.*, 2013). Infrastruktur yang fleksibel dengan mudah mengintegrasikan perangkat baru, mengubah protokol komunikasi, atau menyesuaikan operasi sesuai dengan perubahan lingkungan atau kebutuhan bisnis. Fleksibilitas memungkinkan infrastruktur IoT untuk tetap relevan dan efisien dalam menghadapi perubahan teknologi dan pasar.

Contoh Fleksibilitas dalam Infrastruktur IoT:

Pertimbangkan platform smart home yang dapat mengontrol perangkat rumah seperti lampu, kipas angin, dan perangkat lainnya. Infrastruktur yang fleksibel akan memungkinkan penambahan perangkat baru tanpa perlu

mengubah seluruh sistem, serta memungkinkan integrasi dengan protokol komunikasi yang berbeda sesuai dengan perangkat yang digunakan.

Dalam pengembangan infrastruktur IoT, skalabilitas dan fleksibilitas perlu dipertimbangkan sejak awal. Kedua konsep ini membantu memastikan bahwa solusi IoT dapat tumbuh dan berkembang sejalan dengan perkembangan teknologi dan kebutuhan pasar. Dengan memiliki infrastruktur yang skalabel dan fleksibel, organisasi dapat menghindari kendala dalam mengelola pertumbuhan yang cepat dan perubahan yang tak terduga dalam ekosistem IoT.

3.8 Arsitektur Referensi IoT

Arsitektur Referensi IoT adalah kerangka kerja konseptual yang digunakan untuk merancang dan mengembangkan solusi IoT dengan struktur yang terorganisir dan terstruktur (Bera, Misra and Vasilakos, 2017). Arsitektur ini memberikan panduan tentang bagaimana komponen-komponen dalam ekosistem IoT harus berinteraksi dan bekerja sama secara efisien. Tujuannya adalah untuk menciptakan kerangka kerja yang memungkinkan integrasi yang lebih mudah antara perangkat keras, perangkat lunak, jaringan, dan komponen lainnya dalam solusi IoT.

Arsitektur Referensi IoT umumnya terdiri dari beberapa lapisan (*layers*) yang membentuk struktur berjenjang. Lapisan pertama adalah lapisan perangkat keras (*hardware*), yang mencakup berbagai perangkat sensor, aktuator, dan node komputasi yang mengumpulkan dan mengirimkan data. Lapisan kedua adalah lapisan konektivitas, dimana data dari perangkat keras diarahkan melalui jaringan yang sesuai, seperti jaringan nirkabel atau jaringan seluler. Lapisan ketiga adalah lapisan manajemen data, yang bertanggung jawab untuk menyimpan, mengelola, dan menganalisis data yang dihasilkan oleh perangkat IoT. Lapisan ini penting untuk memahami tren dan pola yang

mungkin memiliki nilai bisnis atau informasi penting. Dengan memiliki kerangka kerja yang jelas seperti ini, pengembang dapat merancang solusi IoT yang lebih efektif dan terukur.

3.8.1 Gambaran Model Arsitektur Referensi

Gambaran Model Arsitektur Referensi adalah sebuah representasi visual yang menggambarkan struktur konseptual dan komponen utama dalam desain dan implementasi solusi IoT. Tujuan dari gambaran ini adalah untuk memberikan pandangan holistik tentang bagaimana berbagai elemen dalam ekosistem IoT saling berinteraksi dan bekerja bersama untuk menciptakan solusi yang efisien dan terintegrasi.

Model Arsitektur Referensi umumnya terdiri dari beberapa lapisan atau komponen utama yang mewakili fungsi-fungsi kunci dalam solusi IoT (Atzori, Iera and Morabito, 2010):

1. Lapisan Perangkat Keras (Hardware Layer): Lapisan paling dasar yang mencakup semua perangkat fisik dalam solusi IoT. Ini termasuk sensor untuk mengumpulkan data dari lingkungan fisik, aktuator untuk memberikan respons, dan perangkat komputasi untuk mengolah data.
2. Lapisan Konektivitas (Connectivity Layer): Lapisan ini menangani komunikasi antara perangkat IoT. Ini melibatkan teknologi komunikasi seperti Wi-Fi, Bluetooth, jaringan seluler, atau protokol khusus seperti Zigbee atau LoRa. Lapisan ini memastikan perangkat dapat berkomunikasi dan berbagi data dengan lancar.
3. Lapisan Manajemen Data (Data Management Layer): Pada lapisan ini, data yang dikumpulkan dari perangkat IoT dikelola, disimpan, dan diolah. Ini melibatkan penyimpanan data dalam sistem basis data atau cloud, pengolahan data untuk analisis, serta penerapan kebijakan keamanan dan privasi data.
4. Lapisan Aplikasi (Application Layer): Lapisan teratas adalah tempat di mana solusi IoT sebenarnya diimplementasikan. Ini mencakup berbagai jenis aplikasi

seperti pemantauan lingkungan, kendali otomatis, analisis bisnis, sistem rumah pintar, kesehatan digital, dan banyak lagi. Lapisan ini berfokus pada cara data dan informasi yang dihasilkan oleh perangkat IoT digunakan untuk memberikan nilai tambah kepada pengguna atau organisasi.

5. Model Arsitektur Referensi membantu dalam merancang solusi IoT yang lebih terstruktur, mudah diatur ulang, dan lebih mudah untuk dikelola. Ini juga membantu dalam mengidentifikasi dan memahami interaksi antara berbagai komponen, serta memastikan bahwa solusi yang dihasilkan dapat berkembang seiring berjalannya waktu.

3.9 Studi Kasus

IoT mencakup berbagai komponen teknologi yang bekerja bersama-sama untuk menghubungkan dan mengumpulkan data dari perangkat fisik, mengirimkan data ke platform yang dapat dianalisis, dan mengambil tindakan berdasarkan informasi yang diberikan oleh data tersebut. Berikut adalah beberapa studi kasus penerapan infrastruktur IoT dalam berbagai industri beserta penjelasannya:

1. Manufaktur: Pabrik Otomotif Toyota

Toyota menggunakan infrastruktur IoT untuk memonitor dan mengoptimalkan rantai pasokan mereka. Mereka memiliki sensor yang terpasang pada mesin produksi dan peralatan pabrik yang mengumpulkan data produksi secara real-time. Data ini digunakan untuk memprediksi perawatan mesin, mengidentifikasi potensi masalah, dan mengoptimalkan efisiensi produksi. Sebagai contoh, sensor dapat mendeteksi keausan pada komponen mesin sehingga perawatan dapat dilakukan sebelum terjadi kegagalan, mengurangi downtime yang tidak terduga.

2. **Kesehatan: Rumah Sakit Cedars-Sinai**
Rumah sakit Cedars-Sinai di Los Angeles menggunakan sensor IoT untuk memantau pasien dengan penyakit kronis. Mereka memberikan pasien perangkat yang mengukur parameter seperti tekanan darah, kadar oksigen, dan detak jantung. Data ini dikirimkan secara langsung ke sistem rumah sakit, memungkinkan tenaga medis untuk memantau pasien jarak jauh dan merespons perubahan kondisi dengan cepat. Hal ini membantu mengurangi jumlah kunjungan ke rumah sakit dan memperbaiki perawatan pasien.
3. **Pertanian: Pertanian Vertikal AeroFarms**
AeroFarms menggunakan sistem IoT dalam pertanian vertikal mereka. Mereka memasang sensor di berbagai lapisan tanaman untuk memantau suhu, kelembaban, pencahayaan, dan nutrisi tanaman. Data ini digunakan untuk mengatur lingkungan tumbuh yang ideal dan memberikan nutrisi yang tepat pada tanaman. Dengan mengoptimalkan kondisi tumbuh, mereka dapat menghasilkan hasil panen yang lebih tinggi dengan lebih sedikit penggunaan air dan tanah.
4. **Energi: Pemantauan Jaringan Listrik Schneider Electric**
Schneider Electric menggunakan IoT untuk memantau jaringan listrik dan peralatan energi. Mereka memasang sensor pada transformator, panel listrik, dan peralatan lainnya. Data yang dikumpulkan membantu dalam mendeteksi gangguan atau ketidaknormalan dalam jaringan listrik secara real-time. Hal ini memungkinkan perusahaan untuk merespons dengan cepat untuk mencegah gangguan lebih lanjut dan mengoptimalkan penggunaan energi.
5. **Transportasi: Perusahaan Pengiriman UPS**
UPS menggunakan infrastruktur IoT untuk mengoptimalkan operasi logistik mereka. Mereka memasang sensor pada truk pengiriman untuk melacak lokasi, kondisi pengiriman (seperti suhu bagi pengiriman bahan makanan), dan pola perjalanan. Data ini membantu dalam pengaturan rute yang lebih efisien,

pemantauan pengiriman yang akurat, dan penggunaan bahan bakar yang lebih hemat.

Studi kasus di atas adalah contoh bagaimana IoT diterapkan dalam berbagai industri untuk meningkatkan efisiensi, pemantauan, dan pengambilan keputusan yang lebih baik. Implementasi IoT ini membantu organisasi dalam mengoptimalkan operasi mereka dan memberikan layanan yang lebih baik kepada pelanggan.

3.9.1 Implementasi Infrastruktur IoT

Pembelajaran dari implementasi sukses infrastruktur IoT adalah inti dari pertumbuhan dan perkembangan teknologi ini. Beberapa aspek penting yang dapat diambil dari implementasi yang sukses adalah:

1. **Perencanaan Strategis:** Implementasi IoT yang sukses dimulai dengan perencanaan strategis yang matang. Organisasi perlu mengidentifikasi tujuan bisnis yang jelas dan merumuskan rencana taktis untuk mencapai tujuan tersebut.
2. **Kolaborasi Antar Tim:** Implementasi IoT melibatkan berbagai tim, termasuk ahli perangkat keras, perangkat lunak, keamanan siber, dan bisnis. Kolaborasi yang efektif antar tim dapat meningkatkan pemahaman dan keselarasan tujuan.
3. **Pemilihan Teknologi yang Tepat:** Pemilihan perangkat keras, protokol komunikasi, dan platform perangkat lunak yang sesuai dengan kebutuhan spesifik proyek sangat penting. Teknologi yang tepat dapat mempengaruhi skalabilitas, performa, dan biaya keseluruhan implementasi.
4. **Manajemen Data yang Efisien:** IoT menghasilkan volume besar data dari berbagai perangkat. Mengelola, menyimpan, dan menganalisis data dengan efisien adalah

- kunci. Solusi analitik dan penyimpanan yang tepat dapat membantu menghasilkan wawasan berharga.
5. Keamanan dan Privasi: Melindungi data dan infrastruktur dari ancaman siber sangat penting. Penggunaan protokol enkripsi, otentikasi, otorisasi, dan tindakan keamanan lainnya harus diutamakan.
 6. Pengelolaan Energi dan Daya Tahan: Efisiensi energi dan manajemen daya diperlukan untuk memastikan perangkat IoT memiliki umur baterai yang memadai dan beroperasi secara konsisten.
 7. Pengukuran Kinerja dan Optimisasi: Mengukur kinerja infrastruktur IoT secara berkala dan melakukan optimisasi berdasarkan hasil pengukuran tersebut sangat penting untuk menjaga performa dan efisiensi.
 8. Pendidikan dan Pelatihan: Memberikan pelatihan kepada pengguna akhir dan personel teknis tentang penggunaan dan pemeliharaan perangkat IoT dapat meningkatkan adopsi teknologi dan mencegah masalah yang mungkin muncul.
 9. Adaptasi terhadap Perubahan: Lingkungan bisnis dan teknologi terus berubah. Kemampuan untuk mengadaptasi infrastruktur IoT sesuai dengan perubahan ini dapat memberikan keunggulan kompetitif.
 10. Studi Kasus dan Praktik Terbaik: Meneliti studi kasus implementasi IoT yang sukses dan praktik terbaik dari organisasi lain dapat memberikan wawasan berharga dan membantu menghindari kesalahan umum.

Penting untuk diingat bahwa setiap implementasi IoT adalah unik, tergantung pada tujuan bisnis, lingkungan operasional, dan teknologi yang digunakan. Pembelajaran dari implementasi yang sukses dapat membantu mengurangi risiko dan mengoptimalkan manfaat dari teknologi IoT.

DAFTAR PUSTAKA

- Abdmeziem, M.R., Tandjaoui, D. and Romdhani, I. 2016, 'Architecting the internet of things: state of the art', *Robots and Sensor Clouds*, pp. 55–75.
- Alferidah, D.K. and Jhanjhi, N.Z. 2020. 'A review on security and privacy issues and challenges in internet of things', *International Journal of Computer Science and Network Security IJCSNS*, 20(4), pp. 263–286.
- Atzori, L., Iera, A. and Morabito, G. 2010. 'The internet of things: A survey', *Computer networks*, 54(15), pp. 2787–2805.
- Bassi, A. et al. 2013. *Enabling Things to Talk: Designing IoT solutions with the IoT Architectural Reference Model*. Springer Nature.
- Bera, S., Misra, S. and Vasilakos, A. V. 2017. 'Software-defined networking for internet of things: A survey', *IEEE Internet of Things Journal*, 4(6), pp. 1994–2008.
- Bhattacharjee, S. 2018. *Practical Industrial Internet of Things security: A practitioner's guide to securing connected industries*. Packt Publishing Ltd.
- Cao, J., Zhang, Q. and Shi, W. 2018. *Edge computing: a primer*. Springer.
- Elmaghraby, A.S. and Losavio, M.M. 2014. 'Cyber security challenges in Smart Cities: Safety, security and privacy', *Journal of advanced research*, 5(4), pp. 491–497.
- Erl, T., Puttini, R. and Mahmood, Z. 2013. *Cloud computing: concepts, technology & architecture*. Pearson Education.
- Geng, H. 2017. *Internet of things and data analytics handbook*. John Wiley & Sons.
- Kranz, M. 2016. *Building the internet of things: Implement new business models, disrupt competitors, transform your industry*. John Wiley & Sons.
- Kurose, J. and Ross, K. 2010. 'Computer networks: A top down approach featuring the internet'. Pearson Addison Wesley.

- Li, S., Da Xu, L. and Zhao, S. 2018. '5G Internet of Things: A survey', *Journal of Industrial Information Integration*, 10, pp. 1–9.
- Perera, C. *et al.* 2014. 'A survey on internet of things from industrial market perspective', *IEEE Access*, 2, pp. 1660–1679.
- Perros, H.G. 2021. *An Introduction to IoT Analytics*. CRC Press.
- Umar, B. *et al.* 2018. 'Evaluation of IoT device management tools', in *Proc. 3rd Int. Conf. Adv. Comput., Commun. Services (ACCSE)*, pp. 15–21.

BAB 4

MANFAAT INTERNET OF THINGS DALAM KEBERLANJUTAN

Oleh Angga Aditya Permana

4.1 Pendahuluan



Gambar 4.1. Ilustrasi IoT
Sumber : <https://www.vecteezy.com/>

Internet of Things (IoT) telah membawa transformasi besar dalam berbagai aspek kehidupan manusia, termasuk keberlanjutan lingkungan. Dengan memanfaatkan konektivitas dan sensor yang semakin canggih, IoT memungkinkan pengumpulan data secara real-time dari berbagai sumber, memfasilitasi pemantauan dan pengelolaan lingkungan yang lebih efisien dan efektif. Salah satu manfaat utama IoT dalam keberlanjutan adalah dalam pengelolaan sumber daya yang lebih bijaksana. Melalui sensor-sensor yang terpasang pada peralatan dan infrastruktur, organisasi dapat

memantau dan mengontrol penggunaan air, energi, dan bahan dengan lebih tepat, mengurangi pemborosan dan dampak lingkungan yang tidak perlu. Misalnya, sensor pintar pada sistem irigasi pertanian dapat mengukur kelembaban tanah dan kondisi cuaca untuk mengatur pasokan air secara otomatis, menghasilkan pertanian yang lebih efisien dan berkelanjutan. (Rosca *et al.*, 2021)

Selain itu, IoT juga berkontribusi dalam pencegahan kerusakan lingkungan melalui monitoring yang lebih canggih. Sensor-sensor IoT dapat digunakan untuk memantau polusi udara, air, dan tanah, serta mendeteksi perubahan yang mengindikasikan ancaman seperti kebakaran hutan atau pencemaran. Data yang dikumpulkan dapat memberikan peringatan dini kepada pihak berwenang, memungkinkan respons cepat dan tindakan pencegahan yang lebih baik. Dalam konteks konservasi, IoT juga mendukung upaya perlindungan terhadap keanekaragaman hayati dan habitat alam melalui pelacakan hewan liar dan pengumpulan data yang membantu dalam pengambilan keputusan tentang upaya konservasi yang tepat.

Selain manfaat operasional langsung, IoT juga memiliki potensi untuk meningkatkan kesadaran dan partisipasi masyarakat dalam isu-isu lingkungan. Dengan mengumpulkan dan menyajikan data lingkungan secara real-time melalui aplikasi dan platform online, IoT dapat membantu mengedukasi masyarakat tentang dampak aktivitas mereka terhadap lingkungan. Ini dapat mendorong adopsi perilaku berkelanjutan dan mendorong partisipasi dalam inisiatif lingkungan, menggerakkan perubahan positif dalam skala yang lebih luas.

Namun, sementara manfaat IoT dalam keberlanjutan sangat berpotensi, tantangan terkait dengan keamanan data dan privasi harus diatasi dengan serius. Karena IoT melibatkan pengumpulan dan pertukaran data yang luas, perlindungan data pribadi dan sensitif serta potensi risiko keamanan siber harus diatasi dengan baik agar penerapan IoT dalam konteks keberlanjutan tetap bermanfaat dan aman bagi masyarakat dan lingkungan.

Internet of Things (IoT) memiliki potensi besar untuk mendukung keberlanjutan (*sustainability*) melalui berbagai cara. Berikut adalah beberapa manfaat utama IoT dalam konteks keberlanjutan:

1. **Monitoring Lingkungan:** IoT memungkinkan pengumpulan data lingkungan secara real-time, seperti kualitas udara, kualitas air, suhu, dan kelembaban. Data ini dapat membantu dalam pemantauan polusi dan perubahan lingkungan, sehingga tindakan dapat diambil untuk menjaga lingkungan yang lebih bersih dan sehat.
2. **Pengelolaan Sumber Daya:** IoT dapat digunakan untuk mengoptimalkan penggunaan sumber daya seperti air dan energi. Contohnya, sensor dapat mengukur konsumsi air dan energi di gedung-gedung atau pabrik-pabrik, kemudian data ini dapat digunakan untuk mengidentifikasi potensi efisiensi dan mengurangi pemborosan.
3. **Pertanian Berkelanjutan:** IoT dapat membantu dalam pertanian berkelanjutan dengan memantau tanaman, tanah, dan kondisi cuaca. Ini memungkinkan petani untuk mengambil keputusan yang lebih baik dalam penggunaan air, pestisida, dan pupuk, mengurangi dampak lingkungan dan meningkatkan hasil panen.
4. **Pengelolaan Limbah:** IoT dapat digunakan untuk mengoptimalkan pengelolaan limbah dengan memantau level dan komposisi limbah di tempat-tempat seperti tempat pembuangan akhir dan fasilitas daur ulang. Ini membantu dalam pengurangan limbah yang tidak perlu dan dalam memastikan bahwa limbah didaur ulang dengan benar.
5. **Mobilitas Cerdas:** IoT dapat meningkatkan efisiensi transportasi dan mobilitas dengan memungkinkan pengumpulan data dari kendaraan dan infrastruktur jalan. Data ini dapat digunakan untuk mengelola lalu lintas

dengan lebih baik, mengurangi kemacetan, dan merancang sistem transportasi yang lebih ramah lingkungan.

6. **Konservasi Energi:** IoT memungkinkan pengendalian dan pemantauan yang lebih canggih terhadap peralatan dan sistem energi, seperti pencahayaan, pemanasan, pendinginan, dan sistem energi terbarukan. Ini dapat membantu mengoptimalkan penggunaan energi dan mengurangi konsumsi yang tidak perlu.
7. **Pencegahan Bencana Alam:** IoT dapat membantu dalam pencegahan bencana alam dan mitigasi kerusakan yang disebabkan oleh peristiwa seperti banjir, gempa bumi, dan kebakaran hutan. Sensor dapat memberikan peringatan dini dan data real-time kepada petugas pemadam kebakaran atau tim penanggulangan bencana.
8. **Keberlanjutan Perkotaan:** IoT dapat mendukung pengembangan perkotaan yang berkelanjutan dengan memantau lalu lintas, kualitas udara, pencahayaan jalan, dan layanan publik lainnya. Data ini dapat membantu pemerintah kota untuk mengambil keputusan yang lebih baik dalam perencanaan perkotaan.
9. **Pemantauan Hewan Liar:** IoT dapat digunakan untuk melacak dan memantau perilaku hewan liar dalam upaya konservasi. Sensor dapat ditanamkan pada hewan untuk mengumpulkan data mengenai migrasi, kesehatan, dan populasi, yang dapat membantu dalam usaha melindungi spesies yang terancam punah.
10. **Pendidikan dan Kesadaran Lingkungan:** IoT dapat digunakan untuk membantu meningkatkan kesadaran dan pendidikan lingkungan. Data dan informasi yang dikumpulkan oleh IoT dapat digunakan untuk mengedukasi masyarakat tentang dampak aktivitas manusia terhadap lingkungan dan menginspirasi tindakan yang lebih berkelanjutan.

Secara keseluruhan, IoT memiliki potensi besar untuk mendukung tujuan keberlanjutan dengan cara yang inovatif dan efektif. Namun, perlu diingat bahwa penggunaan IoT juga harus mempertimbangkan aspek keamanan data dan privasi agar manfaatnya dapat diwujudkan tanpa mengorbankan nilai-nilai yang penting.

4.2 Peran IoT dalam Memonitoring Lingkungan



Gambar 4.2. Ilustrasi IoT Lingkungan

Sumber : auftechnique.com

Peran *Internet of Things* (IoT) dalam mendukung keberlanjutan dalam konteks monitoring lingkungan sangat signifikan. IoT memungkinkan pengumpulan data secara real-time dari berbagai sensor yang terhubung, memungkinkan pemantauan lingkungan yang lebih akurat, efisien, dan responsif. Berikut adalah beberapa cara di mana IoT mendukung sustainability dalam monitoring lingkungan: (Rosca *et al.*, 2021)

1. Pemantauan Kualitas Udara dan Air: Sensor-sensor IoT yang dipasang di berbagai titik dalam lingkungan dapat mengukur parameter kualitas udara seperti partikel PM2.5, gas polutan, dan kadar oksigen. Data ini memungkinkan identifikasi daerah-daerah dengan kualitas udara buruk

dan membantu otoritas kota dalam mengambil tindakan yang tepat, seperti memberlakukan pembatasan lalu lintas atau memperketat regulasi emisi industri. Demikian pula, sensor air IoT dapat digunakan untuk memantau kualitas air di sungai, danau, atau pantai, membantu mendeteksi pencemaran dan memungkinkan tindakan cepat untuk melindungi ekosistem perairan.

2. **Pemantauan Perubahan Iklim dan Cuaca:** Sensor IoT dapat dipasang di berbagai lokasi untuk memantau suhu, kelembaban, tekanan udara, dan pola cuaca lainnya. Data ini membantu dalam pemodelan perubahan iklim, memahami tren cuaca, dan memprediksi peristiwa cuaca ekstrem seperti badai atau kekeringan. Informasi ini memungkinkan pihak berwenang dan komunitas untuk merencanakan respons yang lebih baik terhadap ancaman lingkungan yang diakibatkan oleh perubahan cuaca.
3. **Pengelolaan Bencana dan Respons Darurat:** IoT memungkinkan pengumpulan data secara real-time selama bencana alam seperti gempa bumi, banjir, atau kebakaran hutan. Sensor-sensor IoT dapat mendeteksi perubahan yang terjadi dan mengirimkan informasi kepada pihak berwenang, memungkinkan respons cepat dan efisien. Selain itu, data yang dikumpulkan dapat membantu dalam rekonstruksi pasca-bencana dan pengambilan keputusan untuk mengurangi risiko bencana di masa depan.
4. **Pemantauan Keanekaragaman Hayati:** IoT mendukung konservasi keanekaragaman hayati dengan cara melacak pergerakan hewan liar atau memonitor kondisi ekosistem tertentu. Sensor-sensor yang ditanam pada hewan atau ditempatkan di habitat alam dapat memberikan wawasan tentang pola migrasi, pola makan, dan interaksi antar spesies. Data ini membantu ilmuwan dan konservasionis dalam mengembangkan strategi perlindungan yang lebih efektif.

5. Pemantauan Penggunaan Lahan dan Deforestasi: Sensor-sensor IoT dapat membantu memantau perubahan penggunaan lahan dan tingkat deforestasi di daerah-daerah tertentu. Data ini dapat digunakan untuk mengidentifikasi daerah-daerah yang mengalami tekanan lingkungan akibat perubahan penggunaan lahan yang tidak berkelanjutan, dan membantu dalam merencanakan tindakan konservasi.

Dengan memanfaatkan konektivitas dan kemampuan analitik IoT, pemantauan lingkungan menjadi lebih akurat, tepat waktu, dan terinformasi. Ini memungkinkan pengambilan keputusan yang lebih baik dalam menjaga keberlanjutan lingkungan, mencegah kerusakan, dan merespons ancaman lingkungan secara lebih efisien.

4.3 Peran IoT dalam Pengelolaan Sumber Daya



Gambar 4.3. Ilustrasi IoT dalam Pengelolaan Sumber Daya.
Sumber : <https://www.mertani.co.id/>

Internet of Things (IoT) memiliki peran yang krusial dalam mendukung keberlanjutan dalam pengelolaan sumber daya. Dengan memanfaatkan konektivitas dan kemampuan sensor, IoT memungkinkan pengumpulan data yang akurat dan real-time tentang penggunaan sumber daya, sehingga memungkinkan pengelolaan yang lebih bijaksana dan efisien. Berikut adalah beberapa cara di mana IoT mendukung sustainability dalam pengelolaan sumber daya: (Rosca *et al.*, 2021)

1. **Pengelolaan Air yang Efisien:** Sensor air IoT dapat dipasang pada peralatan atau infrastruktur yang menggunakan air, seperti irigasi pertanian, bangunan komersial, atau rumah tangga. Data yang dikumpulkan dapat memberikan informasi tentang pola penggunaan air, membantu mengidentifikasi pemborosan, dan memungkinkan otomatisasi sistem pengiriman air yang lebih tepat waktu dan sesuai kebutuhan. Hal ini berkontribusi pada konservasi air yang lebih baik, terutama di daerah-daerah yang mengalami kekeringan atau tekanan air.
2. **Pengelolaan Energi yang Optimal:** Sensor-sensor IoT dapat digunakan untuk memantau penggunaan energi di berbagai lingkungan, mulai dari bangunan komersial hingga industri. Data yang dihasilkan dapat memberikan wawasan tentang pola konsumsi energi dan membantu mengidentifikasi peluang efisiensi, seperti mengoptimalkan penggunaan pencahayaan atau pemanas-pendingin. Dengan menggunakan informasi ini, organisasi dapat mengurangi konsumsi energi berlebih dan mencapai penghematan biaya serta emisi karbon yang lebih rendah.
3. **Manajemen Limbah yang Lebih Baik:** IoT dapat digunakan untuk mengoptimalkan pengelolaan limbah dengan memantau volume, komposisi, dan status limbah di fasilitas daur ulang atau tempat pembuangan akhir. Data ini dapat membantu dalam perencanaan pengumpulan dan pengangkutan limbah yang lebih efisien, serta memastikan

- bahwa limbah didaur ulang dengan benar. Selain itu, sensor IoT juga dapat digunakan untuk memantau kualitas udara dan lingkungan di sekitar tempat pembuangan akhir untuk mengidentifikasi dampak lingkungan yang mungkin.
4. Penggunaan Bahan yang Berkelanjutan: IoT dapat mendukung penggunaan bahan yang lebih berkelanjutan dalam proses produksi dan rantai pasokan. Sensor IoT dapat memantau dan melacak aspek-aspek seperti bahan baku, penggunaan bahan kimia, dan tingkat limbah yang dihasilkan. Informasi ini dapat membantu perusahaan mengadopsi praktik produksi yang lebih ramah lingkungan dan memilih bahan yang lebih berkelanjutan.
 5. Agrisains dan Pertanian Berkelanjutan: IoT memungkinkan pertanian berkelanjutan melalui pemantauan tanaman, tanah, dan cuaca. Sensor-sensor IoT dapat memberikan informasi yang akurat tentang kelembaban tanah, kadar nutrisi, dan kondisi cuaca, sehingga petani dapat mengambil keputusan yang lebih cerdas dalam penggunaan air, pupuk, dan pestisida. Ini mengurangi dampak lingkungan dan meningkatkan hasil panen secara berkelanjutan.

Melalui integrasi IoT dalam pengelolaan sumber daya, organisasi dan komunitas dapat mengoptimalkan penggunaan sumber daya alam yang terbatas dan mengurangi dampak lingkungan. Dengan mengumpulkan data yang akurat dan terus menerus, keputusan yang lebih baik dapat diambil untuk mencapai tujuan keberlanjutan jangka panjang.

4.4 Peran IoT dalam Pertanian Berkelanjutan



Gambar 4.4. Ilustrasi IoT pada Pertanian Berkelanjutan
Sumber : web.iribb.org

Peran *Internet of Things* (IoT) dalam mendukung pertanian berkelanjutan sangat penting dalam menghadapi tantangan global seperti populasi yang terus berkembang dan perubahan iklim. Dengan memanfaatkan konektivitas dan sensor, IoT memungkinkan inovasi yang signifikan dalam praktik pertanian, membantu petani dalam mengelola sumber daya dengan lebih efisien dan berkelanjutan. Berikut adalah beberapa cara di mana IoT mendukung pertanian berkelanjutan: (Rosca *et al.*, 2021)

1. Pemantauan dan Pengelolaan Air yang Tepat: Sensor kelembaban tanah dan cuaca yang terhubung melalui IoT dapat memberikan informasi real-time tentang kondisi tanah dan kelembaban. Hal ini memungkinkan petani untuk mengukur kebutuhan air tanaman dengan lebih akurat dan mengatur irigasi secara efisien. Dengan menghindari kelebihan air atau kekeringan, pertanian dapat menghemat air, energi, dan mengurangi dampak lingkungan.

2. **Pemantauan Pertumbuhan Tanaman:** Sensor-sensor IoT dapat dipasang pada tanaman untuk memantau pertumbuhan, kesehatan, dan produktivitas tanaman. Data ini dapat memberikan informasi tentang nutrisi yang dibutuhkan tanaman dan mengidentifikasi masalah kesehatan tanaman lebih awal, memungkinkan intervensi yang tepat waktu dan mengurangi penggunaan pestisida dan pupuk berlebihan.
3. **Prediksi Waktu Tanam dan Panen:** Dengan data cuaca dan tanah yang diperoleh dari sensor-sensor IoT, petani dapat mengoptimalkan jadwal penanaman dan panen. Ini membantu dalam menghindari risiko cuaca ekstrem atau kondisi yang tidak sesuai, yang pada gilirannya dapat meningkatkan hasil panen dan mengurangi risiko kerugian.
4. **Penggunaan Pupuk yang Tepat:** Sensor-sensor IoT dapat membantu dalam mengukur kadar nutrisi tanah dan memantau kebutuhan pupuk. Hal ini memungkinkan petani untuk memberikan pupuk hanya pada area yang membutuhkan, mengurangi limbah dan pencemaran lingkungan akibat penggunaan pupuk berlebihan.
5. **Pantauan Hama dan Penyakit:** Sensor-sensor IoT dapat mendeteksi keberadaan hama dan penyakit pada tanaman dengan cepat. Data ini dapat memberikan peringatan dini kepada petani, memungkinkan tindakan pengendalian yang tepat waktu dan mengurangi ketergantungan pada pestisida kimia.
6. **Pengurangan Jejak Karbon:** IoT dapat digunakan untuk mengoptimalkan penggunaan energi dalam pertanian, termasuk penggunaan alat dan mesin. Sensor-sensor dapat mengukur penggunaan energi dan memberikan wawasan tentang potensi penghematan energi, seperti penggunaan traktor atau sistem irigasi yang lebih efisien.
7. **Optimalisasi Penggunaan Lahan:** Dengan memantau dan menganalisis data tanah dan cuaca, petani dapat

merencanakan penggunaan lahan dengan lebih cerdas. Ini dapat mencakup rotasi tanaman yang lebih efektif, pemilihan varietas tanaman yang sesuai dengan kondisi lokal, dan pengurangan degradasi tanah.

8. Pertanian Berbasis Presisi: IoT mendukung pertanian berbasis presisi dengan mengumpulkan data yang sangat detail dari berbagai sensor. Data ini dapat digunakan untuk membuat peta visual dari lahan pertanian, memungkinkan petani untuk mengambil keputusan yang lebih tepat dalam pengelolaan tanaman dan sumber daya.

Melalui integrasi IoT dalam praktik pertanian, petani dapat mencapai produktivitas yang lebih tinggi dengan pengelolaan yang lebih berkelanjutan. Teknologi ini membantu dalam mengurangi limbah, mengoptimalkan penggunaan sumber daya, dan meningkatkan ketahanan terhadap perubahan iklim, yang semuanya berkontribusi pada pertanian yang lebih berkelanjutan dan ramah lingkungan.

4.5 Peran IoT dalam Pengelolaan Limbah



Gambar 4.5. Contoh IoT Pengelolaan Limbah. Sumber : microthings.id

Internet of Things (IoT) memainkan peran penting dalam mendukung keberlanjutan dalam pengelolaan limbah, dengan memberikan solusi yang lebih efisien, transparan, dan responsif terhadap tantangan pengelolaan limbah modern. Berikut adalah beberapa cara di mana IoT mendukung sustainability dalam pengelolaan limbah: (Rosca *et al.*, 2021)

1. Pemantauan Real-time: Sensor-sensor IoT dapat dipasang pada berbagai fasilitas pengelolaan limbah, seperti tempat pembuangan akhir, fasilitas daur ulang, dan instalasi pengolahan. Sensor ini memantau volume limbah, komposisi, suhu, dan kondisi lainnya secara real-time. Informasi ini memungkinkan pihak berwenang untuk mengawasi dan merespons kondisi fasilitas dengan cepat, menghindari risiko penumpukan limbah berlebihan atau perubahan yang dapat membahayakan lingkungan.
2. Optimalisasi Pengumpulan dan Pengangkutan: Dengan memanfaatkan sensor dan data real-time, proses pengumpulan dan pengangkutan limbah dapat diatur secara lebih efisien. Penggunaan sensor pada tempat sampah di kota atau area komersial dapat memberikan informasi kepada petugas tentang kapasitas limbah, memungkinkan penjadwalan pengangkutan yang lebih cerdas dan menghindari pemborosan waktu dan sumber daya.
3. Pencegahan Pencemaran Lingkungan: Sensor IoT dapat mendeteksi kebocoran atau tumpahan limbah yang dapat menyebabkan pencemaran lingkungan. Ketika sensor mendeteksi indikasi adanya masalah, notifikasi langsung dapat diberikan kepada petugas untuk mengambil tindakan pencegahan lebih lanjut. Hal ini membantu mencegah kerusakan lingkungan yang disebabkan oleh pencemaran.

4. Daur Ulang yang Lebih Efisien: Sensor IoT dapat digunakan dalam rantai pasokan daur ulang untuk melacak dan memantau pergerakan limbah daur ulang. Data ini memungkinkan pelacakan yang lebih akurat terhadap limbah yang diambil, diproses, dan didaur ulang. Hal ini membantu dalam memastikan bahwa limbah daur ulang digunakan dengan efisien, mengurangi kebutuhan akan bahan mentah baru dan mengurangi dampak lingkungan.
5. Manajemen Energi dan Sumber Daya: Sensor-sensor IoT juga dapat membantu dalam pengelolaan energi dan sumber daya di fasilitas pengelolaan limbah. Misalnya, penggunaan sensor energi dapat memantau penggunaan listrik atau gas, memungkinkan pengelola untuk mengidentifikasi peluang penghematan dan efisiensi.
6. Pemantauan Kualitas Udara: Sensor-sensor IoT dapat dipasang di sekitar fasilitas pengelolaan limbah untuk memantau kualitas udara. Hal ini membantu memantau potensi dampak limbah terhadap lingkungan sekitarnya dan memberikan peringatan dini terhadap polusi udara yang mungkin timbul.
7. Analisis Data dan Pemetaan: Data yang dikumpulkan oleh sensor-sensor IoT dapat dianalisis untuk mengidentifikasi tren dan pola dalam pengelolaan limbah. Informasi ini dapat membantu pengambilan keputusan yang lebih baik dalam merencanakan strategi pengelolaan limbah yang lebih berkelanjutan di masa depan.

Dengan memanfaatkan teknologi IoT, pengelolaan limbah dapat menjadi lebih efisien, terukur, dan ramah lingkungan. Solusi-solusi ini membantu mengurangi dampak limbah pada lingkungan, meningkatkan manajemen limbah, dan mendukung tujuan keseluruhan keberlanjutan.

mengurangi emisi gas rumah kaca dan menghemat bahan bakar.

2. **Penggunaan Transportasi Berbagi:** IoT mendukung penggunaan transportasi berbagi seperti sepeda berbagi, mobil berbagi, atau layanan taksi berbasis aplikasi. Sensor-sensor pada kendaraan ini memungkinkan pelacakan lokasi, ketersediaan, dan kondisi kendaraan secara real-time. Pengguna dapat dengan mudah menemukan, menggunakan, dan membayar layanan ini melalui aplikasi, yang dapat mengurangi jumlah kendaraan pribadi di jalan, mengurangi polusi udara dan kemacetan.
3. **Transportasi Publik yang Lebih Efisien:** IoT dapat meningkatkan efisiensi transportasi publik dengan memberikan informasi real-time kepada penumpang tentang jadwal, rute, dan ketersediaan transportasi. Sensor pada kendaraan transportasi publik dapat melacak lokasi dan kepadatan penumpang, sehingga layanan dapat diatur sesuai dengan permintaan yang aktual. Ini membantu mengurangi waktu tunggu penumpang, merangsang penggunaan transportasi umum, dan mengurangi jumlah kendaraan pribadi di jalan.
4. **Kendaraan Otomatis dan Terhubung:** Kendaraan yang terhubung (*connected vehicles*) dan otonom (*autonomous vehicles*) berkomunikasi satu sama lain dan dengan infrastruktur jalan melalui IoT. Hal ini memungkinkan kendaraan untuk berbagi informasi tentang kondisi lalu lintas, cuaca, dan kejadian di jalan. Dengan memanfaatkan informasi ini, sistem dapat menghindari kecelakaan, mengoptimalkan rute, dan mengurangi waktu perjalanan.
5. **Pemantauan Kualitas Udara dan Emisi:** IoT dapat membantu memantau kualitas udara dan emisi kendaraan di berbagai lokasi perkotaan. Sensor-sensor pada kendaraan atau di sepanjang jalan dapat mengukur emisi gas berbahaya seperti nitrogen dioksida dan partikel

PM2.5. Data ini membantu pemantauan kualitas udara dan dapat digunakan oleh pemerintah kota untuk mengatur regulasi kendaraan dan area lalu lintas, serta mengurangi dampak negatif terhadap kesehatan manusia.

6. Pengelolaan Parkir yang Efisien: Sensor-sensor IoT dapat digunakan dalam pengelolaan parkir cerdas. Sensor yang terpasang di tempat parkir dapat memberikan informasi real-time tentang ketersediaan tempat parkir kepada pengendara melalui aplikasi. Hal ini mengurangi waktu yang dihabiskan untuk mencari tempat parkir, mengurangi emisi gas buang akibat berkendara di sekitar untuk mencari parkir, dan mengoptimalkan penggunaan ruang parkir.

Melalui penggunaan IoT dalam mobilitas cerdas, kota dan komunitas dapat mencapai transportasi yang lebih efisien, aman, dan ramah lingkungan. Teknologi ini membantu mengurangi kemacetan, emisi gas rumah kaca, dan polusi udara, serta mendorong adopsi transportasi berkelanjutan yang lebih hemat energi.

4.7 Peran IoT dalam Konversi Energi



Gambar 4.7. Ilustrasi IoT dalam Konversi Energi. Sumber : www.linknet.id

Internet of Things (IoT) memiliki peran kunci dalam mendukung keberlanjutan dalam konversi energi, terutama dalam hal memaksimalkan efisiensi energi, mengintegrasikan sumber energi terbarukan, dan mengelola konsumsi energi dengan lebih cerdas. Berikut adalah beberapa cara di mana IoT mendukung *sustainability* dalam konversi energi:

1. **Pengelolaan Energi Terbarukan:** IoT dapat memantau dan mengoptimalkan kinerja sumber energi terbarukan seperti panel surya, turbin angin, dan sel bahan bakar. Sensor-sensor pada peralatan energi terbarukan dapat mengukur output energi, kinerja, dan kondisi peralatan. Informasi ini memungkinkan pengelolaan yang lebih baik, termasuk pemeliharaan preventif yang tepat waktu dan pengaturan

operasi untuk memaksimalkan produksi energi terbarukan.

2. Distribusi Energi yang Efisien: IoT dapat digunakan dalam pengelolaan jaringan listrik yang cerdas (*smart grids*). Sensor-sensor pada jaringan listrik dapat mengukur beban, tegangan, dan arus pada titik-titik tertentu. Dengan informasi ini, jaringan listrik dapat diatur secara dinamis untuk mengoptimalkan distribusi energi dan mengurangi kehilangan energi yang tidak perlu selama transportasi.
3. Pemantauan Konsumsi Energi: Sensor-sensor IoT dapat dipasang pada bangunan, peralatan, dan sistem untuk memantau penggunaan energi secara real-time. Data ini dapat membantu pengguna untuk mengidentifikasi sumber-sumber pemborosan energi dan mengadopsi tindakan penghematan. Misalnya, sistem penerangan pintar dapat mengatur pencahayaan berdasarkan kehadiran manusia atau tingkat cahaya alami, mengurangi konsumsi energi yang tidak perlu.
4. Manajemen Kualitas Energi: Sensor-sensor IoT dapat memantau kualitas energi seperti tegangan, frekuensi, dan distorsi harmonisa. Informasi ini penting untuk menjaga stabilitas jaringan listrik dan mencegah gangguan atau kerusakan pada peralatan elektronik sensitif. Dengan memastikan kualitas energi yang baik, dapat mengurangi kerugian energi dan perbaikan peralatan yang lebih sering.
5. Penggunaan Baterai yang Efisien: Sensor-sensor IoT dapat membantu mengoptimalkan penggunaan baterai dalam penyimpanan energi. Dalam sistem penyimpanan energi (seperti baterai rumah atau mobil listrik), sensor dapat memantau status baterai, suhu, dan kondisi lainnya untuk memaksimalkan masa pakai baterai, efisiensi, dan kinerja.
6. Integrasi Otomatis Sumber Energi: IoT dapat mengintegrasikan berbagai sumber energi, termasuk sumber energi terbarukan dan penyimpanan energi.

Sensor-sensor dapat mendeteksi ketersediaan sumber energi dan permintaan energi, dan mengatur distribusi dan penggunaan sumber energi dengan cerdas. Ini membantu dalam meningkatkan pemanfaatan sumber energi terbarukan dan mengurangi ketergantungan pada bahan bakar fosil.

7. Manajemen Keseimbangan Energi: IoT dapat membantu dalam manajemen keseimbangan antara konsumsi dan produksi energi. Sensor-sensor dapat memantau konsumsi energi dan memprediksi permintaan masa depan berdasarkan tren dan pola. Dengan informasi ini, sumber energi dapat diatur untuk memenuhi permintaan dengan lebih efisien, mengurangi pemborosan dan risiko *overloading*.

Dengan memanfaatkan IoT dalam konversi energi, kita dapat mencapai penggunaan energi yang lebih efisien, berkelanjutan, dan hemat karbon. Teknologi ini membantu mengoptimalkan produksi, distribusi, dan konsumsi energi, mengarah pada sistem energi yang lebih ramah lingkungan dan berkontribusi pada tujuan keberlanjutan global.

4.8 Peran IoT dalam Pencegahan Bencana Alam



Gambar 4.8. Ilustrasi IoT dalam Pencegahan Bencana Alam
Sumber : getradius.id

Internet of Things (IoT) memainkan peran kunci dalam mendukung keberlanjutan dalam pencegahan bencana alam dengan memberikan kemampuan pemantauan, prediksi, dan respons yang lebih baik terhadap ancaman alam. Berikut adalah beberapa cara di mana IoT mendukung sustainability dalam pencegahan bencana alam: (Ayeni *et al.*, 2010)

1. Pemantauan Lingkungan: Sensor-sensor IoT dapat dipasang di berbagai lokasi untuk memantau kondisi lingkungan seperti cuaca, suhu, kelembaban, dan gempa bumi. Data yang dikumpulkan dari sensor ini dapat memberikan peringatan dini tentang potensi ancaman alam seperti badai, banjir, atau gempa bumi. Informasi ini

memungkinkan pihak berwenang dan masyarakat untuk mengambil tindakan pencegahan atau evakuasi lebih awal.

2. **Pemantauan dan Prediksi Banjir:** Sensor-sensor IoT dapat digunakan untuk memantau tingkat air di sungai, danau, atau area rawan banjir lainnya. Data yang dikumpulkan dapat digunakan untuk memprediksi potensi banjir dan memberikan peringatan dini kepada masyarakat. Selain itu, sistem cerdas berbasis IoT juga dapat mengontrol pintu air dan pompa banjir secara otomatis untuk mengurangi dampak banjir.
3. **Deteksi Dini Kebakaran Hutan:** Sensor-sensor IoT dapat dipasang di hutan atau daerah rawan kebakaran untuk mendeteksi perubahan suhu, kelembaban, dan tingkat kebakaran. Data yang dikumpulkan dapat memberikan peringatan dini kepada petugas pemadam kebakaran dan memungkinkan respons cepat untuk mengendalikan kebakaran sebelum menjadi besar dan sulit dikendalikan.
4. **Pemantauan dan Prediksi Tanah Longsor:** IoT dapat digunakan untuk memantau perubahan kelembaban tanah dan kondisi geologi. Data ini dapat membantu dalam pemantauan dan prediksi potensi tanah longsor, yang dapat menyebabkan kerusakan fisik dan mengancam keselamatan manusia. Peringatan dini melalui sensor IoT dapat memungkinkan evakuasi tepat waktu dan tindakan mitigasi.
5. **Manajemen Evakuasi dan Respons:** IoT dapat digunakan untuk mengatur rute evakuasi yang lebih aman dan efisien selama bencana alam. Sensor-sensor pada jalan dan area publik dapat memberikan informasi real-time tentang kondisi lalu lintas dan rute yang dapat diambil. Selain itu, komunikasi IoT juga memungkinkan pemantauan dan koordinasi respons bencana yang lebih baik antara pihak berwenang, petugas penyelamat, dan warga.

6. Pemantauan Lingkungan Maritim: Sensor-sensor IoT dapat digunakan untuk memantau kondisi laut, termasuk perubahan suhu permukaan laut, tinggi gelombang, dan arus. Data ini dapat membantu dalam memprediksi dan memantau potensi tsunami dan badai laut, serta membantu pihak berwenang dalam memberikan peringatan dini kepada masyarakat pesisir.
7. Sistem Peringatan Dini Multisensor: IoT dapat mengintegrasikan berbagai jenis sensor untuk sistem peringatan dini yang lebih kuat. Sensor cuaca, gempa bumi, tingkat air, dan lainnya dapat saling berkomunikasi dan memberikan informasi yang lebih komprehensif tentang ancaman alam yang mungkin terjadi.

Melalui penerapan IoT dalam pencegahan bencana alam, kita dapat meningkatkan kemampuan kita untuk merespons dan mengurangi dampak dari bencana-bencana alam yang sering terjadi. Teknologi ini membantu dalam mengoptimalkan pemantauan, memungkinkan respons cepat, dan mendukung upaya pencegahan yang lebih efektif, yang semuanya berkontribusi pada tujuan keberlanjutan global.

4.9 Peran IoT pada Pendidikan dan Kesadaran Lingkungan



Gambar 4.9. Ilustrasi IoT pada Pendidikan dan Kesadaran Lingkungan
Simber : ayied.net

Internet of Things (IoT) memainkan peran penting dalam mendukung keberlanjutan dalam pendidikan dan kesadaran lingkungan dengan memberikan alat dan solusi yang inovatif untuk meningkatkan pemahaman, partisipasi, dan tanggung jawab masyarakat terhadap isu lingkungan. Berikut adalah beberapa cara di mana IoT mendukung sustainability dalam pendidikan dan kesadaran lingkungan: (Ayeni *et al.*, 2010)

1. Pendidikan Interaktif: IoT memungkinkan pengembangan pendidikan yang lebih interaktif dan berbasis pengalaman. Melalui sensor dan perangkat terhubung, siswa dapat belajar tentang lingkungan dan keberlanjutan melalui simulasi, visualisasi, dan permainan edukatif yang menarik. Contohnya, sensor-sensor cuaca dapat memungkinkan siswa memahami konsep cuaca dan iklim dengan data yang aktual.
2. Pemahaman Lingkungan: IoT dapat memberikan akses langsung ke data lingkungan dan alam secara real-time. Sensor-sensor di alam liar atau area perkotaan dapat mengumpulkan informasi tentang kualitas udara, suhu, kelembaban, dan lainnya. Data ini dapat diintegrasikan ke dalam kurikulum pendidikan untuk membantu siswa memahami dampak aktivitas manusia terhadap lingkungan.
3. Partisipasi Siswa: IoT dapat memungkinkan partisipasi aktif siswa dalam pengumpulan data dan penelitian lingkungan. Mereka dapat mengumpulkan data tentang flora, fauna, atau polusi udara di sekitar mereka menggunakan perangkat terhubung, dan kemudian menganalisis data tersebut dalam konteks pelajaran. Hal ini memungkinkan siswa untuk terlibat langsung dalam penelitian lingkungan dan pengambilan keputusan.
4. Pengembangan Kesadaran: IoT dapat digunakan untuk meningkatkan kesadaran dan pemahaman masyarakat tentang isu-isu lingkungan. Melalui sensor-sensor yang dipasang di tempat umum atau dalam aplikasi perangkat mobile, masyarakat dapat menerima informasi tentang kualitas udara, tingkat polusi, atau ketersediaan energi terbarukan. Informasi ini membantu mengedukasi masyarakat tentang dampak aktivitas sehari-hari terhadap lingkungan.

5. Pendidikan Jarak Jauh dan Online: IoT memungkinkan pengembangan pendidikan lingkungan jarak jauh atau online dengan menggunakan perangkat terhubung. Siswa dari berbagai belahan dunia dapat mengakses konten pendidikan tentang keberlanjutan dan lingkungan melalui platform digital. Ini membantu menjangkau lebih banyak individu dan meningkatkan pemahaman global tentang isu lingkungan.
6. Pemantauan Energi dan Penggunaan Sumber Daya: IoT dapat digunakan dalam pendidikan tentang efisiensi energi dan penggunaan sumber daya. Sensor-sensor pada gedung sekolah atau kampus universitas dapat memantau konsumsi energi, air, dan lainnya. Siswa dapat belajar tentang cara mengurangi jejak karbon dan mengambil tindakan praktis untuk menghemat sumber daya.
7. Inovasi dalam Pendidikan Lingkungan: IoT dapat menginspirasi inovasi dalam pendidikan lingkungan dengan memanfaatkan teknologi terkini. Penggunaan perangkat wearable seperti jam tangan pintar atau sensor lingkungan portabel dapat memberikan pengalaman pembelajaran yang berbeda, memungkinkan siswa untuk terlibat dalam eksplorasi langsung lingkungan sekitar mereka.

Melalui integrasi IoT dalam pendidikan dan kesadaran lingkungan, kita dapat menciptakan generasi yang lebih sadar lingkungan, terampil dalam penggunaan teknologi berkelanjutan, dan siap mengatasi tantangan lingkungan di masa depan. Teknologi ini membantu dalam merangsang minat, partisipasi, dan pemahaman terhadap keberlanjutan dan konservasi alam.

DAFTAR PUSTAKA

- Ayeni, R.. *et al.* 2010. *National Open University of Nigeria Course Code: Cit101 Course Title: Computers in Society Course.* National Open University of Nigeria.
- Rosca, M.I. *et al.* 2021. 'Internet of Things (IoT) and Sustainability', *BASIQ INTERNATIONAL CONFERENCE Internet*, (January), pp. 346–352. Available at: <https://doi.org/10.24818/basiq/2021/07/044>.

BAB 5

INTERNET OF THINGS DALAM INDUSTRI 4.0

Oleh Melissa Indah Fianty

5.1 Pendahuluan

Proses transformasi teknologi, yang membawa perubahan signifikan dalam struktur ekonomi, budaya, dan sosial manusia, dikenal sebagai Revolusi Industri. Kemajuan dalam teknologi selama 200 tahun terakhir bertanggung jawab atas perubahan dari sistem industri tradisional dan telah mengarahkan evolusi sistem manufaktur pintar, pabrik pintar, layanan kesehatan pintar, praktik pertanian pintar, dan mobil otonom. Berbagai teknologi, seperti Kecerdasan Buatan, robotika, Internet of Things (IoT), pencetakan 3D, nanoteknologi, dan komputasi kuantum, telah mengarah pada pengembangan banyak sistem canggih. Perbaikan-perbaikan bertahap dalam teknologi ini telah menghasilkan Revolusi Industri keempat, yang juga dikenal sebagai Industry 4.0.

Sebagai contoh, dalam generasi Industry 4.0, sistem mandiri seperti derek, kapal, kendaraan otonom yang dipandu secara otomatis, node sensor, bahan baku, dan produk akan berkomunikasi di pelabuhan yang dilengkapi dengan teknologi canggih. Sistem sentral akan membantu logistik dan perangkat lain untuk berkoordinasi dan berkomunikasi di antara mereka guna mengurangi waktu tunggu untuk pemuatan-ankatan kontainer. Oleh karena itu, penggabungan keseluruhan teknologi canggih yang berbeda di bidang komputasi, jaringan, dan proses fisik, dengan integrasi konektivitas Internet di antara proses-proses tersebut, mendorong pengembangan *Cyber-Physical Systems* (CPS). Sistem-sistem ini beroperasi dan berinteraksi dengan dunia fisik secara

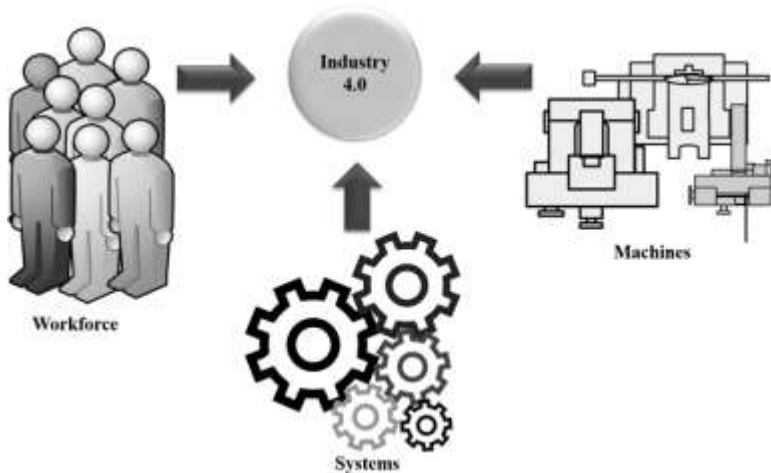
real-time. Komponen-komponen CPS dikembangkan oleh manusia, termasuk pemrosesan, komunikasi, dan pengendalian informasi.

Industry 4.0 adalah singkatan untuk digitalisasi di industri (Jeschke et al., 2017). Selanjutnya, untuk menghadapi perubahan cepat di seluruh dunia, transformasi digital sektor-sektor tersebut dapat menjadi solusi. Digitalisasi ini direpresentasikan sebagai keadaan seni terkini dan disebut sebagai Industry X.0. Gelombang inovasi teknologi telah membawa perubahan luas di industri-industri. Di sisi lain, konektivitas dan interoperabilitas di antara perangkat heterogen memungkinkan komunikasi *Machine-to-Machine* (M2M), yang meningkatkan keamanan mesin dan pekerja. Mesin-mesin pintar mampu mendeteksi kesalahan dalam sistem dan mengambil tindakan korektif yang sesuai. Berkat komunikasi M2M, sebagian besar pekerjaan berbahaya dilakukan oleh mesin. Oleh karena itu, risiko kesehatan yang dihadapi pekerja berkurang secara signifikan. Selain itu, hal ini mengurangi waktu henti mesin dan meningkatkan efisiensi keseluruhan dan kinerja sistem.

Integrasi node sensor pintar, perangkat lunak, teknologi komunikasi dan jaringan, layanan cloud, dan sistem penyimpanan membentuk Industrial Internet. *General Electric* (GE), salah satu anggota pendiri *Industrial Internet Consortium* (IIC), menciptakan istilah Industrial Internet pada akhir tahun 2012. Tiga faktor kunci dari Industrial Internet adalah mesin cerdas dan saling terhubung, analisis kompleks dari jumlah data yang besar yang dihasilkan, dan tenaga kerja yang terhubung. Pasar global *Internet of Things* Industri (IIoT) diperkirakan akan tumbuh sebesar 8,06% per tahun dari tahun 2018 hingga 2023, meliputi berbagai industri seperti manufaktur, minyak dan gas, layanan kesehatan, transportasi, logistik, dan pertambangan. Selain itu, munculnya rantai pasokan real-time meningkatkan pasar IIoT melalui pelacakan pasar, bahan, dan peralatan. Namun, pertumbuhan pasar IIoT masih terbatas oleh masalah keamanan yang terkait dengan Big Data dan AI (Stojmenovic, 2015).

5.2 Industri 4.0

Industry 4.0 adalah istilah yang digunakan untuk tren teknologi saat ini, seperti otomatisasi, pertukaran data di antara perangkat yang saling terhubung, dan interoperabilitas. Industry 4.0 juga disebut sebagai Revolusi Industri keempat. Selain itu, Industry 4.0 menggabungkan berbagai teknologi pendukung ke dalam proses manufaktur industri seperti CPS, komputasi awan, dan IoT. Interoperabilitas di antara berbagai proses, perangkat, data yang terkumpul, dan pemrosesan data secara real-time dari node sensor adalah faktor utama yang diperhatikan selama evolusi Industry 4.0. Gambar 5.1 mengilustrasikan kombinasi dari mesin-mesin heterogen, tenaga kerja (manusia), dan sistem dalam industri. Industry 4.0 memperkenalkan teknologi berbasis Internet untuk meningkatkan komunikasi di antara sistem-sistem. Komunikasi di antara perangkat, sistem, dan mesin yang saling terhubung secara kolektif mengarah pada terbentuknya Industry 4.0.



Gambar 5.1. Industri 4.0
(Sumber : (Misra et al., n.d.))

Karakteristik desain penting dari Industry 4.0 adalah sebagai berikut:

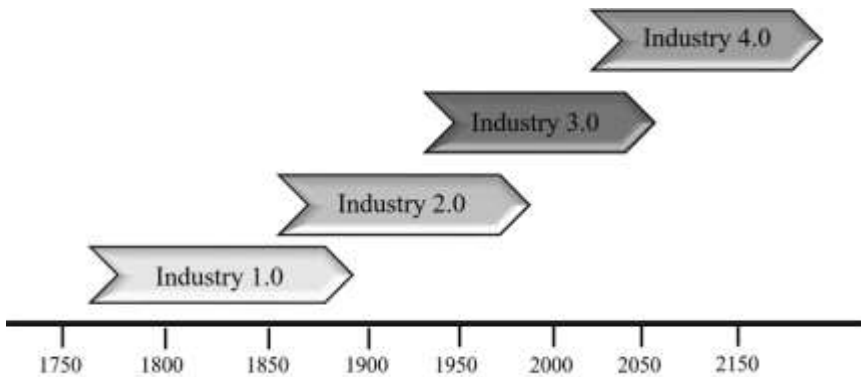
1. Perangkat heterogen seperti node sensor, aktuator, perangkat, dan mesin saling terhubung dan diberikan identifikasi unik melalui teknologi berbasis Internet. Selain itu, perangkat-perangkat yang saling terhubung ini memungkinkan interoperabilitas untuk membentuk jalur produksi yang didukung oleh Industry 4.0.
2. Sistem informasi menggabungkan data mentah dari sensor dan menciptakan salinan virtual dari pabrik fisik dengan menggunakan data yang terkumpul.
3. Sistem-sistem yang saling terhubung dapat berkomunikasi di antara mereka, menjalankan tugas-tugas kompleks secara real-time, dan membuat keputusan dengan sangat sedikit atau tanpa campur tangan manusia. Pekerjaan-pekerjaan yang dilakukan oleh mesin mungkin tidak aman untuk manusia.
4. Sistem-sistem ini mendukung manusia dengan mengumpulkan, memproses, dan menganalisis data yang diterima dari node sensor untuk menghasilkan keputusan sendiri.

Dari sudut pandang sejarah, revolusi industri telah mentransfer pergeseran teknologi manusia dari pemeliharaan hewan hingga pengembangan teknologi di industri. Meskipun berbagai revolusi industri dimulai bertahun-tahun yang lalu, efek revolusi tersebut terhadap ekonomi, struktur sosial, pendidikan, kedokteran, dan budaya berlangsung lama dan signifikan. Revolusi industri juga ditandai dengan munculnya model bisnis baru, arsitektur referensi, modifikasi pada sistem manufaktur, rantai pasokan, dan transportasi.

5.2.1 Revolusi industri: Phases of development

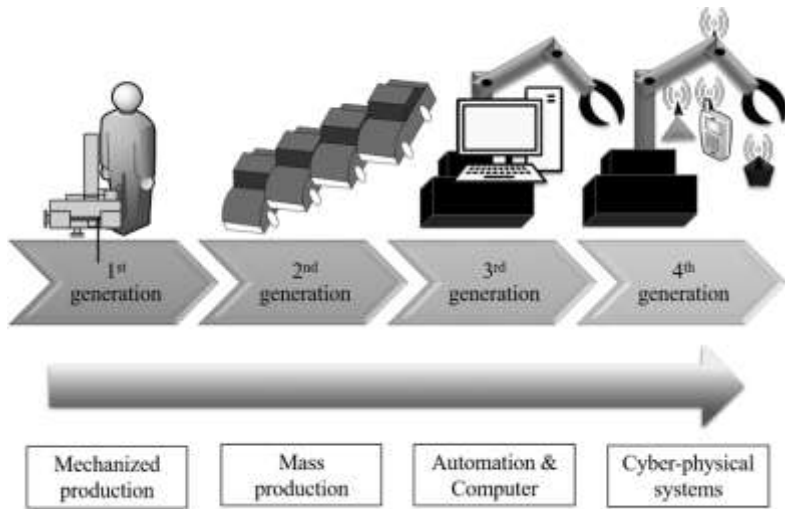
Revolusi Industri telah menghasilkan perkembangan ekonomi dan struktur sosial yang menyeluruh dalam berbagai fase. Seperti yang ditunjukkan dalam Gambar 5.2, revolusi industri pertama dimulai pada abad ke-18. Pada awal abad ke-21, revolusi industri keempat secara resmi dimulai. Dengan kemajuan dalam perkembangan industri, tahapan perkembangan mesin dari generasi pertama hingga sistem berbasis cyber-physical pada generasi keempat ditunjukkan dalam Gambar 5.3. Evolusi revolusi industri pertama terjadi di Britania Raya, di mana para pengusaha menjadi pelopor dari perkembangan teknologi yang tiba-tiba ini. Setelah itu, produksi massal memainkan peran kunci selama revolusi industri kedua. Kemunculan revolusi industri ketiga menyebabkan evolusi teknologi komunikasi nirkabel. Selanjutnya, sekitar abad ke-20, smartphone muncul dengan fasilitas panggilan video terintegrasi. Revolusi industri juga mengakibatkan transfer pengetahuan di antara para pekerja yang terkait dengan inovasi-inovasi ini.

Revolusi Industri Pertama: Transformasi pertama dalam peradaban manusia terjadi dari mencari makan menjadi praktik pertanian, yang dimulai sekitar 10.000 tahun lalu. Langkah awalnya adalah penjinakan hewan untuk pertanian, produksi, dan transportasi. Dari tahun 1750 hingga 1840, teknologi-teknologi baru muncul dalam proses manufaktur. Revolusi industri pertama ditandai dengan peralihan dari tenaga otot menjadi mesin, seperti yang digambarkan dalam Gambar 5.3. Selain itu, efisiensi pembangkitan tenaga air juga meningkat selama periode ini. Proses manufaktur industri baru dan produksi besi dikembangkan pada periode ini. Revolusi industri pertama membuka jalan menuju perkembangan teknologi seperti mekanisasi penggulungan kapas dengan bantuan uap, peningkatan efisiensi mesin uap, dan pengurangan biaya bahan bakar produksi besi dan besi cor. Charles Babbage, dikenal sebagai bapak komputer, menemukan komputer mekanik pertama, pada periode tahun 1822–1834.



Gambar 5.2. Fase-Fase Perkembangan Revolusi Industri.
(Sumber : (Misra et al., n.d.))

Revolusi Industri Kedua: Dua bentuk energi populer yang digunakan sepanjang revolusi industri kedua adalah bensin dan listrik. Salah satu tren teknologi kritis dan mencolok yang berkembang selama revolusi kedua adalah produksi massal. Terinspirasi dari sistem katrol di rumah-rumah pemotongan hewan di Amerika Serikat, Henry Ford mendirikan perusahaan Ford Motor Company. Kemudian, jalur perakitan diterapkan dalam industri manufaktur, yang mengurangi jumlah pekerja yang diperlukan untuk menyelesaikan pekerjaan tertentu. Selain itu, dana juga dikumpulkan untuk kesejahteraan sosial, yang meningkatkan kondisi kesehatan massa masyarakat. Pada tahap-tahap berikutnya, dari tahun 1980 hingga 1990, teknologi komunikasi nirkabel pertama (1G) berkembang. Telepon seluler yang dikembangkan pada masa itu berukuran besar, dengan kualitas suara dan daya baterai yang buruk.



Gambar 5.3. Revolusi Industri.
(Sumber : (Misra et al., n.d.))

Revolusi Industri Ketiga: Dengan dimulainya abad ke-20, revolusi industri ketiga dimulai. Otomasi dalam sistem manufaktur, komputer, Internet, dan penggunaan energi terbarukan adalah beberapa kemajuan dalam teknologi yang terjadi selama revolusi industri ketiga. Oleh karena itu, revolusi ini juga dikenal sebagai Revolusi Komputer atau Digital. Setelah revolusi industri kedua, pengembangan komputer berbasis tabung hampa dimulai. Selanjutnya, komputer pintar dengan sirkuit terpadu dan mikroprosesor muncul pada periode ini. Ponsel pintar juga berkembang di pasaran, dilengkapi dengan fasilitas 3G. Generasi ke-3 atau 3G didefinisikan dengan peningkatan bandwidth, komunikasi yang lebih cepat, dan fasilitas panggilan video. Fasilitas bisnis juga meningkat dengan dimulainya insourcing dan outsourcing. Oleh karena itu, proses yang disebut globalisasi dimulai. Globalisasi menghubungkan perdagangan dan aktivitas

budaya serta meningkatkan produksi barang dan jasa secara keseluruhan di seluruh dunia.

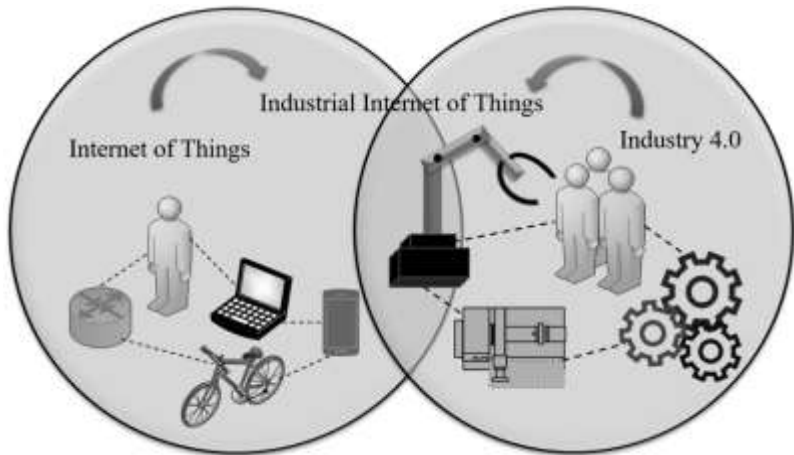
5.2.2 Evolusi Industri 4.0

Penggunaan digitasi yang luas dan teknologi berbasis Internet merupakan ciri khas utama dari Industry 4.0. Revolusi industri keempat ini disebut sebagai Industry 4.0 (Schwab, 2016). Berbagai fitur dari Industry 4.0 adalah sebagai berikut:

1. Integrasi berbagai teknologi seperti Kecerdasan Buatan, komputasi kuantum, sekuensing gen, realitas tambahan dan virtual, teknologi komunikasi nirkabel generasi ke-5 (5G), dan pencetakan 3D membentuk pijakan menuju evolusi Industri 4.0. Teknologi-teknologi ini membentuk fondasi untuk pabrik pintar, mesin-mesin pintar dan terhubung, dan sistem manufaktur pintar.
2. Kerangka dasar teknologi berbasis Internet adalah node sensor pintar. Node sensor pintar berkembang menjadi lebih kuat, lebih murah, dan lebih kecil ukurannya dibandingkan dengan node sensor tradisional.

Integrasi *Internet of Things* (IoT) dan Industri 4.0 membantu munculnya IIoT (*Industrial Internet of Things*), seperti yang digambarkan dalam Gambar 5.4. Perangkat, mesin, dan benda-benda yang terhubung diidentifikasi dengan pengenalan unik dan dikombinasikan dengan mesin-mesin otomatis. Jaringan terhubung dari benda-benda ini membentuk fondasi dasar IIoT. Dengan kata lain, penerapan IoT di industri membuka jalan bagi munculnya IIoT. Di sisi lain, teknologi komunikasi nirkabel 5G merupakan fitur kunci bagi Industry 4.0 dan IIoT. Teknologi 5G ini ditandai dengan kecepatan tinggi, transmisi data yang lebih cepat, mendukung multimedia interaktif, dan streaming suara. Perubahan teknologi secara keseluruhan akan memiliki dampak besar pada seluruh ekologi bisnis. Selanjutnya, integrasi teknologi canggih ini

dengan sistem otomatisasi yang ada akan memulai proses digitalisasi massal di industri.



Gambar 5.4. IoT dan Industri 4.0.
(Sumber : (Misra et al., n.d.))

Profesor Erik Brynjolfsson (Direktur) dan Andrew McAfee (*Principal Research Scientist*) dari *Massachusetts Institute of Technology* (MIT), *Center for Digital Business*, mencetuskan istilah *Second Machine Age* untuk kemajuan terbaru dalam daya komputasi, teknologi komunikasi, dan penyimpanan data (Vemuri, 2014). Mesin-mesin pintar era ini mampu melakukan berbagai tugas yang dapat dilakukan manusia, sehingga mengurangi jumlah tenaga kerja yang diperlukan di lantai pabrik. Oleh karena itu, Revolusi Industri keempat dapat disebut sebagai *Second Machine Age*. Bahan-bahan baru yang tahan lama dan lebih ringan sedang dikembangkan dan diproduksi selama revolusi ini. Berbagai fitur dari era ini meliputi pemrosesan, penyimpanan, dan analisis Big Data, komunikasi M2M di industri, keamanan mesin dan pekerja, konektivitas antara perangkat dan benda, serta keamanan data.

5.2.3 Dampak lingkungan dari revolusi industri

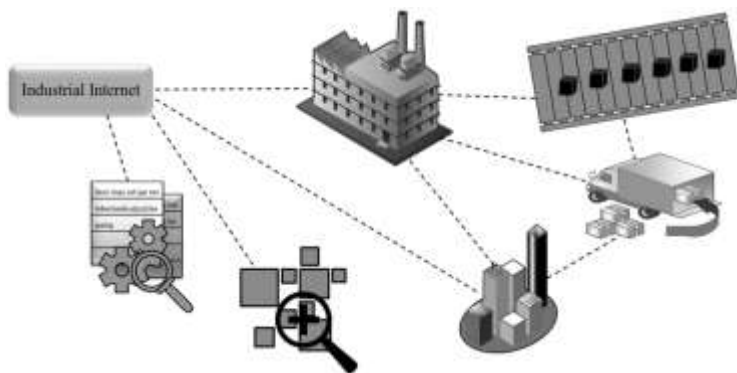
Revolusi industri telah membawa perubahan yang luar biasa dalam teknologi dan penggunaan energi. Di sisi lain, dampak dari revolusi industri ini menyebabkan peningkatan tingkat polusi global, yang mengakibatkan degradasi lingkungan yang signifikan. Selain itu, dengan munculnya mesin-mesin, polusi udara meningkat. Mesin-mesin uap dan berbagai proses industri menggunakan batu bara, yang mengeluarkan jumlah asap dan polutan yang sangat besar. Hal ini meningkatkan tingkat polusi udara, terutama di wilayah-wilayah industri. Selain itu, hasil-hasil kimia yang sangat beracun dari berbagai proses industri dibuang ke badan-badan air, yang menyebabkan polusi air. Gas-gas beracun dan limbah yang dibuang ini memicu degradasi lingkungan. Penggunaan bahan bakar fosil juga meningkat dengan munculnya revolusi industri. Akibatnya, terjadi penipisan yang signifikan dari sumber daya alam terbatas secara global. Dampak besar lainnya dari industrialisasi adalah pemanasan global. Asap yang dihasilkan dari industri bersama dengan gas rumah kaca berbahaya lainnya yang dilepaskan ke atmosfer menyebabkan pemanasan global.

5.2.4 Industrial Internet

Istilah "*Industrial Internet*" pertama kali digunakan oleh perusahaan Amerika Serikat, GE. Industrial Internet merupakan hasil gabungan antara dunia fisik dan digital. Seperti yang didefinisikan oleh GE, Industrial Internet adalah "konvergensi sistem industri global dengan kekuatan komputasi canggih, analitik, sensor berbiaya rendah, dan tingkat konektivitas baru yang diperbolehkan oleh Internet." Konsep dasar dari Industrial Internet diilustrasikan dalam Gambar 5.5. Organisasi yang menerapkan Industrial Internet menggunakan node sensor, perangkat lunak, dan komunikasi *Machine-to-Machine* (M2M) untuk mengumpulkan data dari benda atau perangkat material. Seperti yang ditunjukkan dalam Gambar 5.5, perangkat-perangkat yang saling terhubung di industri, jalur perakitan otomatis, data

real-time yang dikumpulkan dari node sensor, dan analisis data dapat disebut sebagai Industrial Internet. Data yang diolah dan dianalisis menyediakan layanan tambahan bernilai (Soni & Makwana, 2017). Industrial Internet akan menyebabkan peningkatan kecepatan dan efisiensi di berbagai industri seperti penerbangan, kereta api, pertambangan, pembangkitan listrik, dan sistem perawatan kesehatan. Selain itu, ini akan menyebabkan peningkatan fasilitas kerja, mempercepat produktivitas sistem manufaktur, dan mendorong pertumbuhan ekonomi menyeluruh. Dengan kata lain, industri akan memiliki manajemen peralatan, proses, dan sistem yang dioptimalkan dan terpusat. Menurut GE, ada tiga fase dalam perkembangan Industrial Internet, yaitu:

1. Revolusi Industri: Selama revolusi industri pertama dan kedua, produktivitas dan mekanisasi pabrik-pabrik dimulai. Efisiensi pembangkitan tenaga air, pengembangan mesin uap, dan pengurangan biaya bahan bakar terjadi selama revolusi industri pertama. Dengan munculnya jalur perakitan selama revolusi industri kedua, produksi massal dimulai. Selain itu, komunikasi nirkabel menggunakan telepon seluler dikembangkan pada tahap-tahap berikutnya selama periode ini.
2. Revolusi Internet: Revolusi industri ketiga mengarah pada pengembangan otomasi dalam sistem manufaktur, komputer, dan munculnya internet (*World Wide Web*). Revolusi ini juga dikenal sebagai Revolusi Komputer atau Digital. Salah satu efek paling mencolok dari revolusi ini adalah pertukaran informasi secara jarak jauh melalui internet dan smartphone.
3. Industrial Internet: Penggabungan CPS dan evolusi teknologi berbasis internet mengarah pada pengembangan Industrial Internet. Oleh karena itu, umumnya diasumsikan bahwa Industry 4.0 atau revolusi industri keempat berkembang dari teknologi-teknologi ini.



Gambar 5.5. Industrial Internet
(Sumber : (Misra et al., n.d.))

Intelligent machines, advanced analytics, dan connected people adalah elemen kunci di balik perkembangan Industrial Internet. Interkoneksi di antara elemen-elemen kunci ini dan kombinasi mereka meningkatkan ekonomi secara keseluruhan melalui optimalisasi proses, pengurangan biaya produk, dan analisis data real-time. Data real-time membantu memberikan wawasan yang lebih dalam dan meningkatkan operasi sistem di berbagai sektor industri. Faktor-faktor pendorong di balik perkembangan Industrial Internet adalah sebagai berikut:

1. Investasi dalam penyebaran node sensor, perangkat yang diperlukan, proses bisnis, dan antarmuka aplikasi pengguna yang diperbarui akan mendorong perkembangan teknologi baru.
2. Keamanan informasi sensitif, data, dan *intellectual property* (IP) memerlukan sistem keamanan yang kuat.
3. Untuk memacu pertumbuhan bakat baru seperti studi teknik lanjutan, ilmuwan data, dan ahli perangkat lunak mendukung perkembangan industri.

5.2.5 Aplikasi di Industri 4.0

Industry 4.0 adalah integrasi jaringan manusia, benda, mesin, perangkat, dan robot yang saling berinteraksi dan berbagi informasi di antara mereka. Jaringan ini mendigitalkan sistem manufaktur dan menganalisis data real-time yang tersedia dengan CPS (Jeschke *et al.*, 2017). Efisiensi produk meningkat dalam hal waktu dan biaya, kualitas, dan produktivitas keseluruhan meningkat. Selain itu, interoperabilitas di antara benda-benda adalah salah satu fitur utama dari Industry 4.0. Berbagai aplikasi dari Industry 4.0 adalah sebagai berikut:

1. *Smart Factory and Manufacturing system*: Dengan perkembangan teknologi canggih seperti kecerdasan buatan (AI) dan pembelajaran mesin, daya saing di pasar, risiko yang terkait dengan kegagalan, dan peningkatan produksi membantu dalam pengembangan sistem pabrik pintar. Perangkat pintar, teknik pintar, teknologi informasi, analisis data kompleks, dan inovasi adalah komponen-komponen berbeda dari pabrik pintar. Pabrik pintar dan sistem manufaktur mengurangi biaya produksi, meningkatkan efisiensi keseluruhan, meningkatkan keamanan, dan meningkatkan kualitas produk.
2. *Smart Product*: Industry 4.0 mencakup berbagai teknologi seperti CPS, *Information and Communication Technologies* (ICT), IoT, dan integrasi data berbasis cloud untuk membantu manusia dan benda-benda berkomunikasi di antara mereka. Teknologi canggih ini, bersama dengan node sensor pintar, membentuk produk pintar. Selain itu, produk pintar mencakup pengetahuan, informasi, dan sistem produksi real-time yang canggih. Produk pintar dibuat menggunakan proses fisik dan digital yang terhubung.
3. *Smart City: Smart people*, mobilitas pintar, lingkungan pintar, Internet, jaringan sensor, jaringan broadband nirkabel, dan tata kelola pintar menyatu untuk membentuk Kota Pintar. Tujuan utama dari kota pintar adalah

meningkatkan kualitas hidup masyarakat, keselamatan warga, transportasi yang lebih baik dan tepat waktu, serta efisiensi energi yang lebih tinggi. Namun, transformasi dari kota tradisional menjadi kota pintar adalah tugas yang memakan waktu dan rumit.

4. *Lean Production system*: Sistem produksi lean adalah proses pengurangan limbah dalam sistem manufaktur sambil menjaga kualitas produk. Ada tujuh jenis limbah yang terkait dengan sistem manufaktur lean, yaitu inventaris berlebih, pergerakan orang atau informasi, waktu tunggu, aktivitas yang tidak menambah nilai, proses berlebihan, cacat pada produk, dan produksi berlebihan. Dengan adanya Industry 4.0, sistem produksi lean mengidentifikasi limbah, terus meningkatkan kualitas produk, mengurangi biaya produk, dan menambah aktivitas yang menambah nilai. Selain itu, sistem ini juga meminimalkan waktu pengerjaan.
5. *Smart and Connected Business*: Produk pintar dan terhubung meningkatkan efisiensi dan produksi keseluruhan. Dengan menggabungkan model bisnis pintar - proses menjadi lebih murah, efisiensi proses meningkat, dan mencapai pendapatan yang diharapkan. Produk pintar dan terhubung ditandai dengan pemantauan, pengendalian, optimasi, dan otomatisasi. Properti penting dari bisnis pintar dan terhubung adalah pernyataan bisnis yang menambah nilai pada produk, arus pendapatan dari perusahaan atau organisasi, dan teknologi.

5.3 IIoT

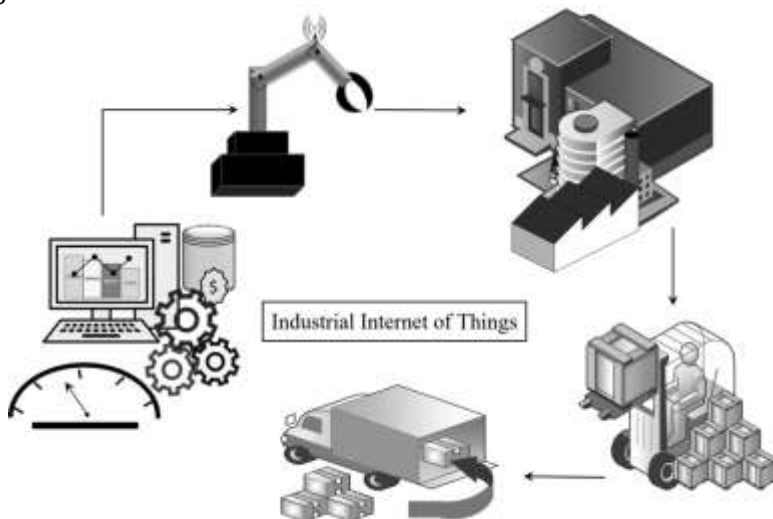
IIoT (*Industrial Internet of Things*) adalah aplikasi berbagai teknologi berbasis IoT, seperti *M2M communication*, *AI*, *Machine Learning*, *Big Data technology*, dan *various automation technologies* di sektor industri (Yilmaz *et al.*, 2017). Fokus utama IIoT adalah

meningkatkan proses manufaktur dan produksi. Perangkat IoT dan IIoT, tingkat otomasi, dan tujuan aplikasi berbeda. IIoT juga dapat disebut sebagai subset yang lebih besar dari IoT. Gambar 5.6 menunjukkan alur kerja dasar di industri yang didukung oleh IIoT. Elemen kunci dari IIoT adalah node sensor pintar, mesin pintar, otomasi, optimasi, dan pemantauan real-time, yang menciptakan transformasi industri. Seperti yang ditunjukkan dalam Gambar 5.6, node sensor yang ditempatkan di berbagai lokasi industri mendeteksi dan mengirimkan data ke server. Pengolahan data secara real-time dan analisis kompleks membantu mengoptimalkan berbagai proses industri seperti pemeliharaan prediktif mesin, manajemen persediaan, dan pengemasan produk jadi. Dengan popularitas teknologi IIoT, node sensor pintar dan prosesor menjadi tersedia dan terjangkau. Selain itu, IIoT bukanlah interkoneksi dari perangkat fisik, tetapi lebih pada digitalisasi produk, proses, dan pabrik. IIC dan GE menyimpulkan bahwa IIoT adalah sinonim untuk Industrial Internet. IIoT menggunakan prinsip-prinsip CPS untuk mendeteksi proses keseluruhan pabrik dan mengambil keputusan otomatis berdasarkan data real-time yang diperoleh. Tujuan utama IIoT adalah meningkatkan efisiensi operasional dan mengoptimalkan biaya, sehingga memodifikasi ulang arsitektur referensi dan model bisnis. Manfaat dari pengemudi IIoT adalah sebagai berikut:

1. Efisiensi operasional dari berbagai proses industri meningkat.
2. Biaya pengembangan produk dan biaya terkait garis perakitan (biaya operasional) berkurang.
3. Waktu henti mesin berkurang, dan energi dapat dihemat. Selain itu, mesin dapat menjadwalkan pemeliharaannya menggunakan analisis prediktif dan preskriptif dari data.
4. Para manajer dan pejabat terkait dapat memantau operasi pabrik dari jarak jauh.

5. Perkiraan yang lebih baik tentang bahan yang tersedia, kemajuan pekerjaan, dan kedatangan persediaan mengarah pada pemanfaatan sumber daya yang maksimal.
6. Keamanan dan keselamatan para pekerja ditingkatkan.
7. Pengalaman pelanggan dan biaya kemasan produk meningkat secara signifikan.
8. Peluang bisnis baru telah diciptakan.
9. Pemantauan secara real-time dari rantai pasokan mengurangi persediaan dan kebutuhan modal.

Oleh karena itu, IIoT umumnya digunakan untuk tujuan industri. IIoT sangat berlaku dalam sektor energi, militer, keselamatan, kesehatan, dan transportasi, di mana keandalan dan akurasi adalah aspek yang penting untuk dijaga. Terdapat beberapa sistem otomasi tradisional yang sudah ada, yang dapat melacak proses produksi secara keseluruhan di dalam pabrik. Namun, IIoT memberikan rincian lebih lanjut tentang kegiatan-kegiatan tersebut.



Gambar 5.6. Industrial Internet of Things
(Sumber : (Misra et al., n.d.))

5.3.1 Prerequisites pada IIoT

IIoT dapat dijelaskan sebagai interkoneksi dari sejumlah besar proses dan sistem industri yang berkomunikasi dan berkoordinasi satu sama lain. Data real-time yang dikumpulkan dari node sensor disimpan, diproses, dan dianalisis untuk meningkatkan kinerja dan efisiensi keseluruhan sistem (Jeschke *et al.*, 2017). Karena dunia digital dan dunia fisik dapat berkomunikasi satu sama lain melalui node sensor dan aktuator, sistem industri telah mendapatkan kemiripan yang erat dengan CPS. Selanjutnya, laten pada jaringan IIoT dijaga dalam kurun waktu kurang dari milidetik, yang sebaliknya dapat menjadi ancaman terhadap kesehatan dan keselamatan mesin dan pekerja. Berbagai persyaratan IIoT (Garbie, 2016) adalah sebagai berikut:

1. Keamanan: Keamanan adalah salah satu aspek penting dari IIoT. Setiap gangguan dalam proses produksi dapat menyebabkan kerugian jutaan dolar. Sebagai contoh, kegagalan dalam smart grid dapat menyebabkan pemadaman listrik di wilayah besar dalam suatu negara. Akibat pemadaman tersebut, jutaan orang terdampak, dan keamanan nasional terancam.
2. Interoperabilitas: Dalam sistem industri, berbagai teknologi seperti Supervisory Control and Data Acquisition (SCADA) dan M2M (Machine-to-Machine) ada bersama-sama untuk menciptakan sistem manufaktur yang canggih. Selain itu, interoperabilitas semantik memungkinkan pertukaran data antara mesin dalam format yang jelas. Namun, interoperabilitas semantik memerlukan interoperabilitas sintaksis untuk mentransmisikan data. Sebagai contoh, transmisi data kesehatan dalam format HL-7 dilakukan untuk menjaga keseragaman dan interoperabilitas data.
3. Skalabilitas: Mesin-mesin, robot, dan kontroler heterogen dihubungkan dalam jumlah besar untuk membentuk jaringan industri. Oleh karena itu, hampir ribuan sensor heterogen dalam jaringan mengumpulkan, menganalisis,

dan memproses data secara kontinu pada saat yang bersamaan. Untuk solusi end-to-end, sinkronisasi di antara komponen sistem diperlukan.

4. Akurasi: Di industri, volume data yang besar dihasilkan setiap milidetik dari perangkat, mesin, dan proses yang terhubung. Sinkronisasi yang tepat dari data yang dikumpulkan sangat penting untuk menjaga kualitas produk. Berdasarkan variasi data, tindakan korektif segera perlu diambil untuk meningkatkan kualitas produk dan efisiensi sistem. (e) Latensi: Dalam setiap proses industri, untuk setiap detik operasional, node sensor mendeteksi dan mentransmisikan data. Dalam hal terjadi anomali yang diamati, data harus diperbaiki melalui pemrosesan otomatis. Jika terjadi penundaan dalam pendeteksian data, pemrosesan, dan eksekusi, hal ini dapat membahayakan keselamatan pekerja, kualitas produk, dan biaya.
5. Keandalan: Di industri, sistem beroperasi dalam kondisi operasi yang berat seperti panas ekstrem, getaran, tekanan, debu, dan dingin, untuk jangka waktu yang lama. Sistem-sistem ini sebagian besar dioperasikan dari jarak jauh oleh operatornya. Oleh karena itu, sistem-sistem ini harus memiliki waktu operasi yang tinggi, toleransi yang lebih besar, dan operasi yang dapat diandalkan selama berjam-jam.
6. Otomatisasi: Sebagian besar proses industri diotomatiskan dari awal hingga akhir operasi, dan memerlukan sedikit atau tidak ada campur tangan manusia. Beberapa teknologi seperti deep learning, logika otomatisasi, proses kontrol, dan berbagai metode analisis data membantu dalam mengintegrasikan kecerdasan ke dalam perangkat-perangkat tepi (edge devices). Selanjutnya, sistem-sistem baru harus mudah diprogram dan diintegrasikan dengan sistem-sistem yang sudah ada.

7. **Servisabilitas:** Node sensor, aktuator, dan protokol membentuk dasar dari setiap sistem industri. Pembaruan firmware diperlukan untuk mengkonfigurasi gateway dan server, mempertahankan tingkat kinerja, dan memenuhi persyaratan pemeliharaan sistem.

5.3.2 Dasar dari CPS

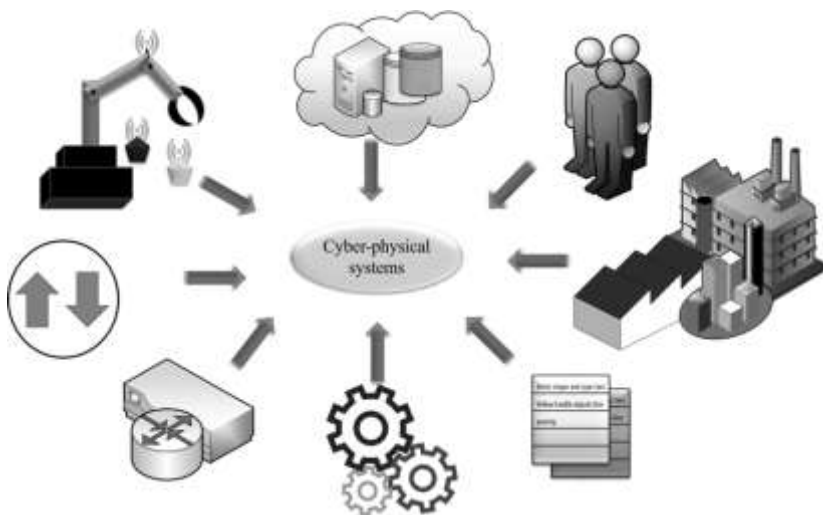
CPS mengintegrasikan objek fisik dan algoritma berbasis komputer, yang saling berkomunikasi dan memperoleh pengetahuan dari lingkungannya. Interkoneksi di antara berbagai objek seperti mesin berbasis sensor, proses, penyimpanan, orang, dan ujung jaringan diilustrasikan dalam Gambar 5.7. Objek fisik dan pengguna terhubung dengan bantuan Internet. Misalnya, prosesor Intel yang dikembangkan pada tahun 1971 memiliki 2300 transistor yang beroperasi pada frekuensi 740 Hz. Di sisi lain, prosesor Intel saat ini memiliki lebih dari 2 miliar transistor, yang beroperasi pada frekuensi sekitar 3 GHz. CPS menggabungkan dan mengkoordinasikan antara elemen fisik dan digital. Karakteristik dari elemen-elemen terkoneksi ini dikategorikan sebagai berikut:

1. **Kemampuan komputasi:** Daya pemrosesan yang lebih tinggi, lebih murah, dan ukuran yang lebih kecil.
2. **Teknologi sensor:** Mendeteksi dan mentransmisikan data dari lingkungan secara real-time.
3. **Keterhubungan di antara elemen-elemen:** Elemen-elemen terhubung dengan teknologi-teknologi berbeda pada saat yang bersamaan dan menerapkan kontrol umpan balik.

CPS tradisional sebagian besar bergantung pada jaringan objek-objek terhubung yang statis. Sistem CPS memiliki beberapa karakteristik dasar seperti masukan-keluaran secara sekuensial, komunikasi di antara banyak proses, kontrol umpan balik real-time berdasarkan data yang dikumpulkan dari node sensor yang terpasang pada mesin-mesin, operasi sinkron dan asinkron, dan berlaku untuk aplikasi kritis keselamatan.

Bentuk lain dari CPS adalah *Mobile Cyber Physical systems*, di mana sistem fisik adalah bergerak. Sumber daya komputasi, radio komunikasi, modul sensor, dan pemrograman tingkat tinggi memungkinkan perangkat seluler dikategorikan sebagai mobile CPS. Mobile CPS telah menjadi populer karena fitur-fitur berikut:

1. Berbagai perangkat masukan-keluaran terhubung, yang berkomunikasi di antara mereka dengan bantuan Internet.
2. Keberadaan perangkat pemrosesan yang signifikan seperti penyimpanan lokal dalam smartphone dan sistem kontrol berbasis umpan balik.
3. Bahasa pemrograman dan logika otomatisasi mendorong perkembangan mobile CPS yang lebih cepat



Gambar 5.7. Cyber-physical systems.
(Sumber : (Misra et al., n.d.))

Kendala utama mobile CPS adalah stabilitas jaringan, kebutuhan daya, keamanan, dan sifat dinamis sistem. Mobile CPS memiliki berbagai aplikasi (Lu, 2017), yang antara lain sebagai berikut:

1. Robot mobile: banyak node sensor pintar, perangkat seluler, dan analisis kompleks membantu meningkatkan efisiensi dan proses tugas yang kompleks.
2. Sistem transportasi cerdas: komunikasi di antara kendaraan dan infrastruktur meningkatkan keamanan dan keamanan kendaraan.
3. Teknologi pintar: kota pintar, sistem kesehatan pintar, dan pemantauan lingkungan membantu meningkatkan keamanan, keamanan, dan mengurangi konsumsi energi.

5.3.3 CPS dan IIoT

CPS mengintegrasikan objek fisik dengan objek digital melalui Internet. Objek digital bertindak secara virtual sebagai mesin fisik. Jaringan dari objek-objek terhubung ini dalam industri manufaktur disebut sebagai IIoT. Oleh karena itu, CPS terhubung yang berlaku di sektor industri disebut sebagai IIoT. Mesin pertama kali terhubung ke server lokal, di mana data yang terdeteksi ditransmisikan. Data yang terdeteksi kemudian dikonversi menjadi data tingkat mesin. Kesehatan adaptif mesin dievaluasi melalui objek virtual yang dibuat secara digital. Kualitas mesin, kondisi, dan kualitas produk diperiksa. Akhirnya, mesin dikonfigurasi berdasarkan data yang diproses.

IIoT adalah infrastruktur yang diperlukan untuk Industri 4.0 atau Revolusi Industri Keempat, CPS, dan IIoT. IIoT memungkinkan pendeteksian jarak jauh dari objek fisik di seluruh jaringan. Selain itu, CPS adalah blok dasar untuk membangun pabrik pintar masa depan. Berbagai bentuk aplikasi berbasis CPS digunakan untuk mengembangkan Industri 4.0. Mesin pintar dapat mengkonfigurasi diri, mengoptimalkan diri, dan dapat menyesuaikan diri dengan fluktuasi mendadak dalam jaringan. Di sisi lain, analitik pintar, pembelajaran mendalam, dan metode pembelajaran mesin memberikan informasi real-time tentang kesehatan mesin dan setiap bentuk penurunan kondisi mesin. Oleh karena itu, CPS industri meningkatkan proses produksi, mengurangi waktu henti,

mengurangi waktu persiapan mesin, meminimalkan kesalahan, dan memberikan respons yang lebih cepat. Kualitas produk meningkat melalui perbaikan terus-menerus menggunakan kontrol berbasis umpan balik dan analitik canggih.

5.3.4 Aplikasi pada IIoT

IIoT memiliki berbagai aplikasi di berbagai industri manufaktur. Penerapan sistem *Computer-Integrated Manufacturing* (CIM) di lantai pabrik telah mengarah pada pengembangan *Product Data Management* (PDM). PDM menjadi dasar bagi *Product Lifecycle Management* (PLM). Di industri, PLM bertindak sebagai antarmuka untuk berbagai aplikasi selama pengelolaan siklus hidup produk. PDM dan PLM adalah persyaratan utama untuk pertumbuhan IIoT (Anghel *et al.*, 2016). Beberapa area aplikasi utama IIoT adalah sebagai berikut:

1. *Smart healthcare* : Jaringan terhubung dari perangkat dan sistem tergantung pada sensor pintar yang baru muncul, perangkat medis, dan sistem. Kondisi kesehatan pasien kritis dapat berfluktuasi kapan saja. Oleh karena itu, pemantauan terus-menerus terhadap pasien sangat penting. Berbagai jenis perangkat pintar dikonfigurasi secara dinamis sesuai kebutuhan pasien. Perangkat realitas tambahan dan virtual membantu dokter selama operasi dan terapi. Tantangan utama dalam pengembangan lebih lanjut dari perangkat ini adalah merancang dan mengembangkan sistem kesehatan yang aman, andal, dan handal. Sistem kesehatan, di mana sensor mendeteksi dan mentransmisikan data fisiologis pasien ke local processing unit (LPU). Selanjutnya, LPU mentransmisikan data ke server lokal. Di sisi lain, para ahli medis seperti dokter, paramedis, dan perawat di rumah sakit dapat mengamati kondisi kesehatan pasien dari jarak jauh.
2. *Smart supply chain* : Informasi cerdas, terkoneksi, dan real-time tentang produk telah mendorong munculnya rantai

pasok pintar. Persyaratan pemeliharaan yang tepat dari bahan baku, stok inventaris yang tersedia, rincian setiap langkah yang terlibat dalam proses produksi, aliran informasi yang baik di antara berbagai tahapan, menjaga jendela waktu pengiriman barang, dan pengembalian barang cacat adalah elemen penting yang terlibat dalam pengembangan rantai pasok pintar. Aliran informasi yang tepat di antara berbagai komponen rantai pasok. Penanganan data real-time, pemrosesan data, dan penyimpanan dilakukan secara sentral di cloud (Sehgal & Bhatt, 2018). Selanjutnya, otomatisasi terlibat dalam berbagai proses gudang seperti pengelolaan inventaris, pembebanan produk, dan distribusi.

3. *Smart Transportation*: Dengan peningkatan pesat jumlah kendaraan di jalan raya, keamanan pengemudi dan kendaraan menjadi isu utama dalam industri transportasi jalan raya. *Intelligent Transportation System* (ITS) dan *Advanced Driver Assistance Systems* (ADAS) telah dikembangkan untuk meningkatkan sistem lalu lintas. Selain itu, teknologi ini telah mengurangi kemacetan di jalan raya, kecelakaan, dan tingkat kematian. Transportasi pintar dan terhubung. Sensor-sensor ditempatkan pada kendaraan dan *Road Side Units* (RSU). Sensor-sensor yang ditempatkan ini mendeteksi dan mentransmisikan data ke server lokal. Berbagai informasi real-time seperti kecepatan aman, jarak aman dengan kendaraan tetangga, dan kondisi cuaca diberikan kepada pengemudi. Selain itu, komunikasi antara kendaraan dan infrastruktur (RSU) meningkatkan keamanan kendaraan, pejalan kaki, dan pengemudi.
4. *Smart manufacturing system* : Untuk meningkatkan efisiensi produksi dan kualitas produk, mengurangi biaya produksi per unit, dan meningkatkan umur mesin dan produk yang dikembangkan, sistem manufaktur pintar dikembangkan. Proses otomatis packaging produk di pabrik manufaktur

dengan sedikit campur tangan manusia. Berbagai sensor ditempatkan di berbagai lokasi, dan robot atau mesin membungkus produk. Seperti yang dapat kita amati, ban konveyor menyesuaikan dan mengirimkan produk sesuai kebutuhan. Di sisi lain, operator dapat memantau seluruh proses dari jarak jauh. Oleh karena itu, sensor pintar, aktuator, dan berbagai algoritma berbasis perangkat lunak membentuk dasar dari sistem manufaktur. Integrasi teknologi ini dan perangkat fisik yang terhubung memungkinkan simulasi, optimasi, dan komunikasi di antara berbagai proses selama periode operasional pabrik. Jaringan di antara perangkat ini dan model virtual membentuk sistem manufaktur pintar.

5. *Smart Grid* : Otomatisasi dan penggunaan energi terbarukan dimulai dengan revolusi industri ketiga. Namun, dengan adanya digitalisasi, efisiensi energi dan produksi listrik telah meningkat. Melalui penjadwalan perangkat, optimasi permintaan, dan otomatisasi terdistribusi, terjadi pengurangan yang signifikan pada beban puncak, gangguan, dan kekurangan daya. Peningkatan perangkat *Flexible AC Transmission* (FACTS) dan *Phasor Measurement Units* (PMU) telah menghasilkan solusi yang lebih baik untuk smart grid.

5.4 Kesimpulan

Bab ini terdiri dari konsep dasar Revolusi Industri Keempat atau Industry 4.0, Industrial Internet, CPS, dan IIoT.

1. Revolusi Industri adalah proses konversi teknologi untuk perubahan struktur ekonomi, budaya, dan sosial manusia.
2. Dengan revolusi industri pertama, proses produksi mekanis berkembang.
3. Selama revolusi industri kedua, produksi massal dimulai.
4. Otomatisasi dalam sistem manufaktur, komputer, dan Internet dimulai pada waktu revolusi ketiga.

5. Kombinasi berbagai teknologi seperti komputasi kuantum, kecerdasan buatan, komunikasi nirkabel generasi ke-5 menghasilkan perkembangan revolusi industri ke-4, atau Industry 4.0.
6. Industry 4.0 memiliki berbagai aplikasi dalam bidang pabrik pintar dan sistem manufaktur, produk pintar, kota pintar, dan sistem manufaktur lean.
7. Istilah Internet Industri diciptakan oleh GE, yang menekankan pentingnya integrasi dunia fisik dan digital.
8. Internet Industri secara luas berlaku di bidang aviasi, transportasi, kesehatan, dan produksi energi.
9. IIoT, yang merupakan subset lebih besar dari IoT, secara utama berfokus pada peningkatan proses manufaktur dan produksi.
10. CPS mengintegrasikan objek-objek fisik dengan algoritma berbasis komputer melalui Internet.
11. IoT adalah blok dasar dari CPS, Industry 4.0, dan IIoT.
12. IIoT secara luas berlaku di berbagai sektor industri seperti kesehatan, transportasi, manufaktur, dan rantai pasokan.

DAFTAR PUSTAKA

- Anghel, A., Vasile, G., Boudon, R., d'Urso, G., Girard, A., Boldo, D., & Bost, V. 2016. Combining spaceborne SAR images with 3D point clouds for infrastructure monitoring applications. *ISPRS Journal of Photogrammetry and Remote Sensing*, 111, 45–61.
<https://doi.org/https://doi.org/10.1016/j.isprsjprs.2015.11.008>
- Garbie, I. 2016. Emerging Issues. In *Green Energy and Technology* (pp. 23–31). Springer Science and Business Media Deutschland GmbH. https://doi.org/10.1007/978-3-319-29306-6_3
- Jeschke, S., Brecher, C., Meisen, T., Özdemir, D., & Eschert, T. 2017. *Industrial Internet of Things and Cyber Manufacturing Systems* (pp. 3–19). https://doi.org/10.1007/978-3-319-42559-7_1
- Lu, Y. 2017. Industry 4.0: A Survey on Technologies, Applications and Open Research Issues. *Journal of Industrial Information Integration*, 6. <https://doi.org/10.1016/j.jii.2017.04.005>
- Misra, S., Roy, C., & Mukherjee, A. (n.d.). *Introduction to Industrial Internet of Things and Industry 4.0*.
- Schwab, K. 2016. *The Fourth Industrial Revolution*. www.weforum.org
- Sehgal, N., & Bhatt, P. 2018. *Cloud Computing*. <https://doi.org/10.1007/978-3-319-77839-6>
- Soni, D., & Makwana, A. 2017. *A SURVEY ON MQTT: A PROTOCOL OF INTERNET OF THINGS(IOT)*.
- Stojmenovic, I. 2015. Fog computing: A cloud to the ground support for smart things and machine-to-machine networks. *2014 Australasian Telecommunication Networks and Applications Conference, ATNAC 2014*, 117–122.
<https://doi.org/10.1109/ATNAC.2014.7020884>

- Vemuri, V. 2014. The Second Machine Age: Work, Progress, and Prosperity in a Time of Brilliant Technologies, by Erik Brynjolfsson and Andrew McAfee. *Journal of Information Technology Case and Application Research*, 16, 112–115. <https://doi.org/10.1080/15228053.2014.943094>
- Yilmaz, İ. G., Aygün, D., & Tanrikulu, Z. 2017. Social Media's Perspective on Industry 4.0: A Twitter Analysis. *Social Networking*, 06(04), 251–261. <https://doi.org/10.4236/sn.2017.64017>

BAB 6

PERAN INTERNET OF THINGS DALAM BISNIS DIGITAL

Oleh Heru Saputra

6.1 Pendahuluan

Dalam era serba digital yang terus berkembang, *Internet of Things* (IoT) telah menjadi landasan penting dalam sebuah bisnis digital. Dengan kemampuan untuk menghubungkan perangkat, mengumpulkan data, dan menganalisis informasi secara real-time, IoT memberikan dampak yang signifikan dalam meningkatkan efisiensi operasional, pengalaman pelanggan, dan memungkinkan inovasi produk dan layanan yang lebih baik. Pada bab ini, kita akan mempelajari dan mengetahui bagaimana Internet of Things menjadi landasan kesuksesan bisnis digital dan mengapa peran pentingnya tidak dapat diabaikan.

6.1.1 Pengenalan Internet of Things (IoT)

Internet of Things (IoT) telah membawa perubahan besar terutama di dunia bisnis digital. Dalam era yang semakin terhubung, IoT mengacu pada jaringan perangkat, kendaraan, dan objek lain yang saling terhubung melalui internet dan memungkinkan pertukaran data yang berkelanjutan. Dalam bisnis digital, IoT berperan sangat penting untuk meningkatkan efisiensi operasional, mengoptimalkan pengalaman pelanggan, dan menghasilkan inovasi produk dan layanan yang revolusioner. Dengan memanfaatkan sensor, perangkat pintar, dan analisis data real-time, pelaku bisnis dapat mengoptimalkan proses produksi, memonitor inventaris, menyesuaikan strategi pemasaran, dan memberikan pelayanan yang lebih baik kepada pelanggan.

IoT juga membawa perubahan yang sangat besar dalam bagaimana cara pelaku bisnis beroperasi. Dengan adanya konektivitas yang luas, pelaku bisnis dapat mengumpulkan dan menganalisis data secara *real-time*, memberikan wawasan berharga yang dapat menginformasikan keputusan bisnis yang lebih cerdas dan strategis. Selain itu, IoT juga memungkinkan pelaku bisnis untuk menggabungkan sistem, perangkat, dan platform yang berbeda menjadi satu ekosistem yang terintegrasi. Sebagai contoh, dalam industri manufaktur, IoT memungkinkan mesin dan peralatan untuk saling berkomunikasi, memantau kinerja, dan mengoptimalkan proses produksi. Sedangkan dalam retail, IoT dapat menghubungkan perangkat, sistem inventaris, dan analisis yang berguna untuk memberikan informasi pembelian yang lebih personal dan efisien kepada pelanggan, dengan hadirnya IoT, bisnis digital memiliki potensi besar untuk menjadi lebih efisien, inovatif, dan kompetitif.

6.1.2 Pengenalan Bisnis Digital

Penggunaan *Internet of Things* (IoT) dalam Bisnis digital mengacu pada penggunaan seperti perangkat, sensor, dan objek lainnya terhubung ke Internet yang memungkinkan pertukaran data secara *real-time*. Pelaku bisnis dapat mengumpulkan dan menganalisis data untuk mengidentifikasi tren, mengoptimalkan proses, dan membuat keputusan dengan tepat, sehingga dapat mengoptimalkan bisnis dan menciptakan nilai tambah bagi pelaku bisnis dan pelanggan. penerapan IoT pada bisnis digital dapat menghadirkan beberapa inovasi-inovasi seperti pintu otomatis yang terbuka saat ada pelanggan yang akan masuk/keluar dari toko, penghematan energi melalui pengaturan otomatis suhu dan pencahayaan, atau bahkan pengiriman barang yang terpantau secara *real-time* melalui sensor. Dengan memanfaatkan IoT, bisnis digital dapat menciptakan pengalaman pelanggan yang lebih personal, meningkatkan efisiensi operasional, dan memberikan nilai tambah yang lebih besar.

6.2 Peran IoT dalam Bisnis Digital

Peran dari IOT dalam bisnis digital, adalah pelaku usaha dapat memperoleh informasi yang lebih akurat dan detail tentang preferensi pelanggan, pola konsumsi, dan tren pasar. Hal ini dapat membantu pelaku usaha mengidentifikasi peluang baru dan mengembangkan strategi pemasaran yang lebih baik dan efektif. Selain itu, IoT juga memungkinkan pelaku usaha mengoptimalkan proses produksi lebih efisien dengan mengotomatiskan proses yang terhubung secara digital.

6.2.1 Meningkatkan Efisiensi Operasional

Meningkatkan Efisiensi Operasional sangat penting bagi pelaku usaha, dengan memanfaatkan IoT pelaku usaha dapat menghubungkan perangkat dan mengumpulkan data secara real time yang sebelumnya dilakukan secara manual. Dengan memanfaatkan IoT pelaku bisnis dapat mengurangi kesalahan yang dilakukan oleh manusia dan mempercepat waktu yang diperlukan untuk menyelesaikan pekerjaan. Misalnya, penerapan IoT di industri manufaktur, IoT dapat digunakan untuk memantau mesin atau peralatan secara otomatis dan memperingatkan pelaku usaha jika terjadi kerusakan atau malfungsi, sehingga mengurangi waktu henti produksi yang tidak terduga (Ahmad dkk, 2016). Selain itu, IoT dapat membantu pelaku usaha mengoptimalkan penggunaan bahan bakar secara lebih efisien. Dengan mengumpulkan data seperti konsumsi energi, suhu dan kelembapan, pelaku usaha dapat mengidentifikasi pola penggunaan yang tidak efisien dan mengambil tindakan yang diperlukan untuk mengurangi konsumsi bahan bakar yang berlebihan atau mempertahankan kondisi yang optimal. Misalnya, di sektor transportasi, IoT dapat digunakan untuk mengoptimalkan rute pengiriman dan mengurangi penggunaan bahan bakar(Sundmaecker dkk, 2010).

6.2.2 Meningkatkan Pengalaman Pelanggan

Dalam meningkatkan pelayanan kepada pelanggan dalam proses bisnis. Pelaku usaha perlu mengumpulkan data tentang preferensi dan kebiasaan pelanggan secara real time, pelaku usaha dapat memberikan interaksi atau layanan yang lebih individual dan dekat dengan pelanggan. Contohnya ada retail misalnya, penggunaan IoT bisa digunakan untuk memberikan rekomendasi produk yang disesuaikan dengan preferensi pelanggan. Dengan menggunakan informasi tentang riwayat pembelian, preferensi warna, atau gaya tertentu, pelaku usaha dapat memberikan pelayanan yang baik bagi pelanggan dalam berbelanja yang dipersonalisasi dan lebih memuaskan (Fang, 2018). Selain itu, penggunaan IoT memungkinkan sebuah pelaku bisnis untuk menyediakan layanan kepada pelanggannya yang lebih responsif. Dengan perangkat IoT memungkinkan perusahaan untuk dapat mengumpulkan data secara real-time tentang produk yang dijualnya terhadap pelanggan. Dengan cara ini, perusahaan dapat memantau dan mengantisipasi potensi cacat atau masalah, memungkinkan tindakan proaktif dan layanan pelanggan yang lebih baik. (Verma, P, 2017)

Selain itu, IoT juga dapat menciptakan interaksi pelanggan dengan menghubungkan perangkat dan menggunakan teknologi seperti *augmented reality* (AR) atau *virtual reality* (VR), pelaku usaha dapat menciptakan pengalaman yang imersif dan interaktif. Misalnya, di industri restoran, IoT dapat digunakan untuk memberikan pelayanan tamu yang interaktif dan personal melalui aplikasi seluler yang terhubung ke perangkat IoT di kamar hotel. (Swan, M, 2012)

6.2.3 Inovasi Produk dan Layanan

Inovasi produk dan layanan merupakan bagian penting dari suatu proses bisnis. IoT, atau *Internet of Things*, telah membuka peluang dan inovasi tanpa batas di dunia bisnis digital. Dengan menghubungkan perangkat dan mengumpulkan data secara real

time memberi kesempatan kepada pelaku usaha untuk mengembangkan produk dan layanan yang lebih baik dan memenuhi kebutuhan pelanggan yang dibutuhkan. Salah satu contoh inovasi produk yang tercipta melalui Internet of Things adalah perangkat smart home. Rumah dapat dikontrol secara otomatis melalui aplikasi smartphone yang menggunakan sensor dan koneksi internet. Hal ini memungkinkan pemilik rumah dengan mudah dan efisien mengontrol mulai dari suhu, pencahayaan, keamanan, dan bahkan sistem pembersihan. Selain itu, Internet of Things juga telah mengubah cara pelaku usaha memberikan layanan kepada pelanggan.

Inovasi produk dan layanan Dari segi bidang medis memungkinkan pemantauan kesehatan jarak jauh berbasis sensor terhadap kesehatan pasien. Hal ini memungkinkan penyedia layanan kesehatan untuk memberikan perawatan yang lebih personal dan real-time serta memantau pasien dengan lebih efisien. Sedangkan di sektor transportasi, *Internet of Things* telah menghadirkan inovasi seperti kendaraan otonom yang dapat berkomunikasi satu sama lain dan dengan infrastruktur jalan. Hal ini tidak hanya meningkatkan keamanan dan efisiensi transportasi, tetapi juga membuka peluang baru untuk pengembangan layanan transportasi berbasis aplikasi dan berbagi kendaraan. Dengan IoT, pelaku usaha juga dapat mengumpulkan informasi berharga tentang perilaku dan preferensi konsumen. Informasi ini dapat digunakan untuk mengidentifikasi tren pasar, menganalisis pola pembelian, dan menciptakan wawasan mendalam untuk mengembangkan produk dan layanan yang memenuhi kebutuhan pelanggan dengan lebih baik. Dengan demikian, Internet of Things telah membuka peluang bagi inovasi tanpa batas dalam perdagangan digital. Dari produk pintar hingga layanan data, IoT menawarkan peluang bagi bisnis untuk mendapatkan keunggulan kompetitif dan memberikan pengalaman pelanggan yang lebih baik.

6.2.4 Peningkatan Keamanan dan Keandalan

IoT, telah membawa perubahan revolusioner dalam keamanan dan keandalan bisnis digital, yang memungkinkan pelaku usaha memantau dan melacak berbagai aspek usahanya secara real time, dan meningkatkan keamanan dan keandalan secara keseluruhan. Salah satu contoh nyata penggunaan IoT untuk meningkatkan keamanan adalah penggunaan kamera pengintai yang terhubung melalui Internet. Dengan koneksi ini, pelaku usaha dapat memantau ruang kerja, mengidentifikasi potensi ancaman keamanan, dan dengan cepat mengambil tindakan yang diperlukan. Selain itu, penggunaan IoT dapat mendeteksi kebocoran gas, kebakaran, atau bahkan gangguan yang tidak diinginkan, memungkinkan respons yang lebih cepat dan perlindungan yang lebih baik terhadap aset dan pekerja. Selain itu, IoT memungkinkan pelaku usaha memantau dan memelihara peralatan atau mesin secara real time. Dengan sensor yang terpasang pada perangkat dapat mengirimkan informasi tentang kondisi dan kinerjanya. Dengan cara ini, perusahaan dapat mengambil tindakan pemeliharaan preventif dan menghindari kerusakan yang tidak terduga. Dengan mengoptimalkan keandalan peralatan, perusahaan dapat menghindari waktu henti yang mahal dan memaksimalkan produktivitas operasional. Selain keamanan dan keandalan internal, *Internet of Things* juga berperan penting dalam menjaga keamanan pelanggan dan kualitas produk. Misalnya, dalam industri makanan, dengan memanfaatkan IoT dapat digunakan untuk memantau suhu dan kelembapan dalam rantai makanan. Hal ini memungkinkan deteksi dini kondisi yang tidak sesuai atau kemungkinan kontaminasi, sehingga memastikan konsumen mendapatkan produk yang aman dan berkualitas tinggi. Berkat IoT, perusahaan dapat menerapkan solusi yang lebih cerdas dan terhubung untuk meningkatkan keamanan dan keandalan bisnis digital. Dari pemantauan keamanan data waktu nyata hingga pemeliharaan proaktif, IoT memberi perusahaan keunggulan

dalam memecahkan masalah keamanan data dan meningkatkan efisiensi operasional secara keseluruhan.

6.3 Implementasi IoT dalam Berbagai Sektor Bisnis

Internet of Things (IoT) telah muncul sebagai pendorong terpenting perubahan digital di berbagai industri. Gagasan bahwa perangkat yang terhubung ke Internet dapat berkomunikasi dan beroperasi secara otomatis telah membuka kemungkinan baru dan menghasilkan inovasi yang mengubah cara bisnis beroperasi dan berinteraksi dengan pelanggan. Dengan adanya IoT dan pemanfaatannya di berbagai sektor seperti transportasi, perawatan kesehatan, dan pertanian yang telah menunjukkan potensi luar biasa mulai dari meningkatkan efisiensi, meningkatkan pelayanan pelanggan, dan menciptakan solusi dan layanan yang cepat.

6.3.1 IoT dalam Retail

Beberapa industri retail yang menerapkan IoT telah menuai banyak keuntungan, seperti: 66% retailer melaporkan bahwa IoT berdampak positif pada proses pelayanan terhadap konsumen dan 88% responden mengatakan bahwa menggunakan IoT pada ritel akan memberikan wawasan konsumen yang lebih baik daripada metode pengumpulan data secara manual. Dengan teknologi IoT ini pelaku usaha dapat mengumpulkan data untuk menentukan perilaku konsumen ke depannya. Berikut beberapa manfaat penerapan IoT dalam sektor retail:

1. Manajemen inventaris: Teknologi IoT memungkinkan pelaku usaha untuk menggunakan sensor yang dapat terhubung untuk memantau semua inventaris barang kapan saja. Dengan adanya IOT dapat memberikan informasi yang akurat tentang ketersediaan dan inventaris produk. Informasi ini dapat membantu pelaku usaha untuk mengoptimalkan manajemen inventaris, mengurangi biaya penyimpanan yang tidak perlu, dan menghindari

kekurangan inventaris yang dapat mengganggu pelayanan pelanggan.

2. Kustomisasi dan rekomendasi produk: Teknologi IoT dapat membantu pelaku usaha lebih memahami preferensi dan perilaku pelanggan. Dengan informasi ini, toko dapat memberikan rekomendasi produk menawarkan beberapa opsi bagi pelanggan untuk memilih. Hal ini dapat membantu meningkatkan kepuasan pelanggan dan meningkatkan peluang penjualan.
3. Pembayaran yang cepat dan aman: Teknologi IoT dapat diterapkan untuk proses pembayara, yang disebut dengan teknologi Near Field Communication (NFC) yang memungkinkan pelanggan untuk melakukan pembayaran dengan cepat dan tanpa kontak fisik. Hal Ini memberikan kemudahan dan kenyamanan bagi pelanggan apabila pelanggan tidak membawa uang secara tunai.
4. Manajemen energi yang efektif: IoT juga dapat digunakan dalam manajemen energi pada sebuah toko. Dengan menggunakan sensor, dan sistem cerdas memungkinkan toko memantau dan mengoptimalkan penggunaan energi seperti lampu dan AC. halIni membantu mengurangi biaya operasi dan dampak lingkungan.
5. Pengambilan keputusan: Dengan mengumpulkan dan menganalisis data yang dihasilkan oleh IoT, toko dapat memperoleh informasi berharga tentang perilaku pelanggan, produk, dan efisiensi operasional. Hal ini memungkinkan pelaku usaha dapat membuat sebuah keputusan yang lebih baik, cepat dan strategis saat menjalankan bisnisnya.

6.3.2 IoT dalam Industri Manufaktur

IoT telah merevolusi industri dengan cepat dan mengintegrasikan perangkat dan sistem terhubung yang memungkinkan pelaku usaha untuk mengoptimalkan proses

produksi, meningkatkan efisiensi operasional, dan meningkatkan prediktabilitas perawatan mesin untuk produktivitas yang lebih besar. Berikut beberapa manfaat penerapan IoT dalam Industri Manufaktur:

1. Pemantauan dan pengoptimalan manufaktur: Dengan menggunakan IoT, industri manufaktur dapat memantau dan mengoptimalkan proses produksi secara real-time dan mengumpulkan semua informasi mulai dari suhu, kelembaban, tekanan, dan parameter lain yang terkait dengan kinerja mesin dan peralatan produksi. Informasi ini dapat digunakan untuk mengidentifikasi potensi masalah atau malfungsi dan mencegah downtime yang tidak diharapkan selama operasional.
2. Pemeliharaan prediktif: Dengan menggunakan IoT, industri manufaktur dapat menerapkan pemeliharaan prediktif berdasarkan kondisi mesin. Dan memantau kinerja mesin dan mendeteksi apabila terjadi kerusakan atau keausan. Dengan analisis data yang akurat, perusahaan dapat merencanakan pemeliharaan tepat waktu dan mencegah kerusakan yang lebih parah. Dengan begitu pelaku bisnis dapat mengurangi biaya tidak terduga dan biaya perbaikan yang tinggi.
3. Manajemen rantai pasok: IoT dapat digunakan untuk melacak dan mengelola data inventaris seperti bahan baku, suku cadang, dan barang jadi. Dengan cara sensor akan dipasang di rak atau palet yang dapat memberikan informasi tentang kesediaan barang. Hal dapat membantu pelaku usaha untuk mengoptimalkan manajemen inventaris, menghindari kekurangan atau kelebihan inventaris, dan meningkatkan efisiensi rantai pasok.
4. Perusahaan yang saling terhubung: Dalam industri manufaktur yang kompleks, IoT memainkan peran yang sangat penting dalam menghubungkan berbagai sistem dan perangkat ke dalam satu perusahaan yang terintegrasi. Hal

ini memungkinkan data untuk ditransmisikan dengan cepat dan akurat antara mesin, peralatan, dan sistem kontrol. Dengan adanya konektivitas yang baik ini, perusahaan dapat meningkatkan koordinasi antar departemen, mengoptimalkan alur produksi, dan mengurangi waktu siklus produksi secara signifikan.

5. **Kualitas Produk yang Lebih Baik:** Dengan penerapan IoT, industri manufaktur dapat meningkatkan kualitas produk secara efektif. Perangkat yang terhubung dapat mengumpulkan semua informasi tentang parameter kualitas seperti dimensi, berat, kekuatan, dan lainnya. Informasi ini kemudian dapat digunakan untuk mendeteksi cacat atau ketidaksesuaian dengan standar kualitas yang telah ditetapkan pelaku usaha. Dengan adanya informasi ini, pelaku usaha dapat meningkatkan kualitas produk, mengurangi tingkat cacat, dan otomatis akan meningkatkan kepuasan pelanggan.

6.3.3 IoT dalam Transportasi dan Logistik

Pada industri transportasi dan logistik IoT berdampak besar dan mengubah cara bagaimana beroperasi. Misalnya, dalam bidang logistik, IoT memungkinkan penggunaan sensor pada kendaraan pengemasan untuk melacak pengiriman paket secara real time. Pelaku usaha/kosumen dapat dengan mudah melacak lokasi barang dan mendapatkan informasi barang sudah sampai mana, tentang suhu, kelembaban, dan kondisi lingkungan lainnya. Hal ini dapat membantu mencegah kerusakan atau kerugian yang tidak diinginkan dan dengan adanya ini dapat meningkatkan kepuasan pelanggan terhadap jasa pengiriman. Berikut beberapa manfaat penerapan IoT dalam Transportasi dan Logistik:

1. **Efisiensi:** Pelaku usaha dapat mengoptimalkan penggunaan sumber daya seperti kendaraan, jadwal pengiriman, dan perawatan mesin. Hal ini dapat mengurangi biaya

- operasional, meningkatkan produktivitas, dan menghindari gangguan yang tidak diinginkan.
2. Andal: Dengan pemantauan secara real-time dan analisis data, pelaku usaha dapat mengidentifikasi masalah secara tepat dan dapat mengambil tindakan yang diperlukan.
 3. Keamanan: IoT dapat menampilkan sebuah informasi tentang situasi lalu lintas, cuaca, atau kondisi jalan berbahaya. Hal ini memungkinkan pengemudi untuk membuat keputusan yang lebih aman dan mengurangi risiko kecelakaan.
 4. Pengurangan Dampak Lingkungan: Dengan menggunakan teknologi IoT pengemudi dapat mengoptimalkan rute pengiriman dan mengurangi emisi gas buang. Ini membantu untuk menjaga kualitas udara dan mengurangi dampak negatif transportasi terhadap lingkungan.
 5. Meningkatkan Kepercayaan Pelanggan: IoT dapat memberikan Informasi real-time tentang lokasi dan status pengiriman, yang disediakan oleh jasa pengirim yang memungkinkan pelaku usaha untuk memberikan pemantauan yang lebih baik kepada pelanggan. Hal ini menciptakan transparansi dan meningkatkan kepuasan pelanggan karena mereka dapat mengikuti perjalanan barang mereka dengan mudah.

6.3.4 IoT dalam Layanan Kesehatan

Duni Kesehatan telah menggunakan teknologi IoT untuk meningkatkan layanan, pemantauan kesehatan dan memberikan perawatan yang lebih baik terhadap pasien. Perangkat yang terhubung seperti sensor dan wearable yang dikenakan pada pasien dapat mengumpulkan data kesehatan pasien secara real-time, hal ini memungkinkan pemantauan jarak jauh dan deteksi perubahan terhadap pasien. Selain itu, IoT memungkinkan pasien untuk berpartisipasi aktif dalam perawatan mereka dengan menggunakan perangkat seluler untuk mengukur tanda-tanda

vital, tingkat aktivitas, dan pola tidur. IoT dapat juga digunakan untuk mengoptimalkan manajemen inventaris dan perawatan medis untuk memastikan ruangan terisi dengan baik dan bersih pada rumah sakit. Penggunaan teknik pembelajaran mesin dan analisis data dalam sistem IoT juga meningkatkan kecepatan dan akurasi diagnosis, memungkinkan identifikasi pola penyakit yang secara tradisional sulit dideteksi, serta mendorong diagnosis dini dan pengobatan yang efektif. Berikut beberapa manfaat penerapan IoT dalam Layanan Kesehatan:

1. Mengontrol kesehatan: Dengan perangkat dan sensor yang terhubung, pasien dapat memantau kesehatannya kapan saja. Hal ini memungkinkan identifikasi dini terhadap perubahan yang signifikan dan memicu tindakan medis yang tepat waktu. Pasien juga dapat memantau tanda-tanda vital dan tingkat aktivitas mereka sendiri, hal ini dapat membantu mereka untuk mengambil langkah-langkah pencegahan yang tepat.
2. Perawatan Pasien: Dengan data yang dikumpulkan melalui IoT, tim medis dapat menganalisis informasi yang lebih komprehensif tentang kondisi pasien. memungkinkan perawatan yang lebih personal dan terukur, dengan penyesuaian yang tepat untuk kebutuhan individu. Hal ini juga memungkinkan perawatan dapat dilakukan jarak jauh atau telemedicine yang menghubungkan pasien dengan dokter tanpa harus hadir secara fisik.
3. Efisiensi Operasional: IoT dapat membantu untuk mengoptimalkan proses operasional dalam layanan kesehatan. Contohnya seperti penjadwalan yang lebih baik, manajemen inventaris yang akurat, dan penggunaan sumber daya yang efisien. Hal ini mengurangi biaya operasional, meningkatkan produktivitas, dan memastikan ketersediaan peralatan dan obat-obatan yang tepat pada waktu yang tepat.

4. **Diagnosis yang Lebih Cepat dan Akurat:** Dengan adanya IoT dapat membantu dokter dalam membuat diagnosis yang lebih cepat dan akurat terhadap pasien. Hal ini membantu mengidentifikasi pola atau tanda-tanda penyakit yang mungkin terlewatkan secara manual. Dengan penerapan IoT Hal ini dapat mempercepat perawatan dan tindakan apa yang harus dilakukan terhadap pasien.
5. **Pencegahan dan Pengendalian:** Melalui pemantauan kesehatan yang terus-menerus dan analisis data, IoT dapat membantu dalam pencegahan dan pengendalian terhadap penyakit kronis pada pasien, pasien dapat menerima peringatan dini atau rekomendasi untuk mengubah gaya hidup mereka. Hal ini membantu mengurangi risiko komplikasi dan meningkatkan kualitas hidup pasien.

6.3.5 IoT dalam Pertanian dan Pangan

Penggunaan IoT pertanian dan industri pangan telah mengubah dari segala aspek baik dari segi pengairan, pemupukan, dan perlindungan tanaman dan penerapan IoT dapat memantau kesehatan hewan, mencegah kontaminasi makanan, dan meningkatkan manajemen inventaris. Berikut manfaat IoT dalam Pertanian dan Pangan:

1. **Monitoring yang lebih baik:** Dengan menggunakan IoT, pemilik lahan dapat memantau kondisi lahan pertaniannya melalui sebuah smartphone, kemudian pelaku usaha mendapatkan informasi seperti tentang suhu, kelembaban, kualitas tanah, dan lain lain. Dengan memanfaatkan IoT dalam bidang pertanian dan pangan, pemilik lahan dengan mudah dan cepat apa yang sedang terjadi di lahan pertaniannya tanpa harus menghabiskan waktu berlama-lama di sana.
2. **Penghematan sumber daya:** peran IoT juga dapat membantu mengoptimalkan penggunaan sumber daya seperti air dan energi. Pelaku usaha dapat mengatur irigasi secara otomatis berdasarkan kondisi tanaman dan pada penerapan di rumah

kaca dapat mengontrol suhu. jadi dengan adanya teknologi IoT pelaku usaha bisa menghemat waktu dan uang, serta menjaga lingkungan.

3. Prediksi dan mitigasi risiko: pelaku usaha dapat menganalisis pola dan apa yang akan terjadi dengan memanfaatkan data yang dikumpulkan oleh IoT. Hal ini akan membantu pemilik lahan dalam memprediksi kemungkinan serangan hama atau penyakit tanaman, serta mengambil tindakan pencegahan yang tepat dan bisa mengurangi risiko kerugian selama panen.
4. Peningkatan efisiensi produksi: dengan bantuan IoT pemilik lahan dapat meningkatkan efisiensi produksi dengan memantau dan mengontrol proses produksi secara otomatis. Sehingga pemilik lahan mendapatkan informasi tentang ketersediaan stok, mengatur pengiriman produk, dan mengoptimalkan rantai pasok.

6.4 Tantangan dan Peluang dalam Mengadopsi IoT dalam Bisnis Digital

Mengadopsi *Internet of Things* (IoT) dalam bisnis digital di Indonesia tidak terlepas dari tantangan yang harus dihadapi. Keamanan dan privasi data menjadi salah satu perhatian utama, sementara keterbatasan infrastruktur teknologi juga perlu diperhatikan, terutama di daerah yang kurang terjangkau. Selain itu, kebutuhan akan sumber daya manusia terampil dan terlatih serta pemahaman dan kepatuhan terhadap regulasi dan kebijakan yang berkaitan dengan IoT menjadi aspek penting dalam mengadopsi teknologi ini. Namun, di balik tantangan tersebut, terdapat peluang besar untuk memanfaatkan IoT dalam bisnis digital di Indonesia. Implementasi IoT dapat meningkatkan efisiensi operasional dalam berbagai sektor bisnis, memungkinkan pengembangan produk dan layanan inovatif yang mengintegrasikan teknologi IoT, dan memberikan pengalaman pelanggan yang lebih baik. Pertumbuhan pasar IoT yang pesat juga

memberikan peluang bagi bisnis untuk meraih keunggulan kompetitif. Dengan kesadaran akan tantangan dan peluang ini, bisnis di Indonesia dapat mencapai kemajuan yang signifikan dalam mengadopsi IoT dalam bisnis digital

6.6 Kesimpulan

Internet of Things (IoT) memiliki peran penting dalam transformasi bisnis digital. Dalam meningkatkan efisiensi operasional, pengalaman pelanggan, inovasi produk dan layanan, serta keamanan dan keandalan, IoT memberikan banyak peluang dalam berbagai sektor bisnis seperti retail, manufaktur, transportasi, layanan kesehatan, dan pertanian. Namun, tantangan seperti keamanan data, keterbatasan teknologi dan infrastruktur, serta kebutuhan sumber daya dan pelatihan perlu diatasi. Dengan strategi yang tepat, bagi para pelaku usaha dapat memanfaatkan potensi IoT dalam mencapai kesuksesan dalam bisnis digital.

DAFTAR PUSTAKA

- Ahmad, R., & Sreenan, C. J. 2016. Internet of Things (IoT): Application of Big Data and Artificial Intelligence. *IEEE*.
- Sundmaeker, H., Guillemin, P., Friess, P., & Woelfflé, S. 2010. *Vision and Challenges for Realising the Internet of Things. Cluster of European Research Projects on the Internet of Things (CERP-IoT)*.
- Lu, Y., Yang, S., Chou, D. C., & Fang, W. 2017. Exploring the Internet of Things (IoT) Consumer Market: A Survey. *IEEE Internet of Things Journal*, 5(2), 759–769. doi: 10.1109/JIOT.2017.2766078
- Verma, P., & Verma, S. 2017. *Internet of Things (IoT) and Its Role in Business*. 20–25. doi: 10.1109/ISS1.2017.8388799
- Swan, M. 2012. Sensor Mania! The Internet of Things, Wearable Computing, Objective Metrics, and the Quantified Self 2.0. *Journal of Sensor and Actuator Networks*, 1(3), 217–253. doi: 10.3390/jsan1030217

BAB 7

INTERNET OF THINGS DALAM KESEHATAN

Oleh Fahmy Rinanda Saputri

7.1 Pendahuluan

Pada masa kini, berbagai teknologi yang beragam memiliki pengaruh terhadap desain sistem di berbagai bidang, seperti *Internet of Things Sosial* (SIoT). IoT dianggap sebagai elemen penting dalam teknologi cerdas seperti jejaring sosial, perawatan kesehatan, sistem siber-fisik, dan mekanisme keamanan (Ortiz *et al.*, 2014). Melalui IoT, benda-benda pintar saling terhubung dan melakukan pertukaran data besar di antara satu sama lain. Data ini kemudian dianalisis melalui berbagai metode dan teknik dalam berbagai penelitian. Analisis utama dari data besar ini bervariasi dari satu bidang ke bidang lain, terutama dalam jejaring sosial. Terdapat berbagai survei yang berfokus pada sistem keamanan dalam perawatan kesehatan dan aplikasi industri. Tantangan dan solusi keamanan sangat terkait dengan sensor jaringan (jaringan sensor nirkabel). Sebenarnya, IoT mampu mengatasi tantangan ini secara lebih efektif daripada solusi konvensional, serta meningkatkan pemanfaatan Internet of Things Sosial (SIoT). Selain itu, aplikasi-aplikasi IoT juga mengalami peningkatan di berbagai bidang lain seperti Internet of Medical Things (IoMT), Internet of Nano Things (IoNT), Internet of Mobile Things (IoMBT), Internet of Cloud Things (IoCT), Internet of Drone Things (IoDT), Industrial Internet of Things (IIoT), dan Internet of Underwater Things (IoUT).

Pada bab ini akan membahas peran *Internet of Things* (IoT) dalam bidang kesehatan dan kedokteran. IoT telah mengubah cara kita memandang sistem perawatan kesehatan dengan menghadirkan solusi inovatif dan efisien. Dengan koneksi yang mulus antara perangkat medis, sensor, dan infrastruktur jaringan, IoT membuka peluang baru untuk pemantauan pasien secara real-time, diagnosis yang lebih cepat, dan pengelolaan penyakit yang lebih baik. Dalam bab ini, akan dijelaskan bagaimana implementasi IoT telah menghadirkan revolusi dalam layanan kesehatan, termasuk penggunaan sensor medis yang terhubung untuk pemantauan pasien, pengembangan perangkat wearable yang dapat memantau kondisi kesehatan, serta pengelolaan data medis besar yang memberikan wawasan berharga bagi penelitian dan pengembangan medis. Selain itu, tantangan keamanan dan privasi yang terkait dengan penggunaan IoT dalam kesehatan juga akan dibahas untuk memastikan keberlanjutan dan penerapan yang aman dalam sektor ini.

Penerapan *Internet of Things* (IoT) telah menghadirkan berbagai manfaat yang signifikan dalam sektor kesehatan, membawa perubahan positif dalam cara kita merawat, memantau, dan meningkatkan kesehatan individu serta masyarakat. Berikut ini adalah beberapa manfaat utama yang dihasilkan oleh pemanfaatan IoT dalam dunia kesehatan:

1. **Pemantauan Kesehatan Real-Time:** IoT memungkinkan pemantauan pasien secara real-time melalui perangkat medis yang terhubung. Data vital seperti tekanan darah, detak jantung, suhu tubuh, dan kadar glukosa dapat terus dipantau dan dikirimkan kepada tenaga medis, memungkinkan deteksi dini masalah kesehatan dan tindakan cepat.
2. **Pengelolaan Penyakit Kronis:** Pasien dengan penyakit kronis dapat diuntungkan dari perangkat wearable yang terhubung dengan IoT. Perangkat ini membantu pasien mengelola penyakit mereka dengan memberikan pemantauan dan peringatan terkait kondisi kesehatan mereka, serta

- memfasilitasi pengiriman data langsung kepada dokter untuk penilaian.
3. Pencegahan dan Prediksi: IoT memungkinkan pengumpulan dan analisis data kesehatan skala besar. Dengan mengintegrasikan informasi dari berbagai sumber, termasuk lingkungan dan perilaku pasien, sistem IoT dapat membantu dalam mengidentifikasi pola dan tren yang dapat mengarah pada pencegahan penyakit atau bahkan prediksi potensi masalah kesehatan.
 4. Perawatan Jarak Jauh (Telemedicine): IoT memfasilitasi pelayanan medis jarak jauh, memungkinkan konsultasi medis, diagnosis, dan tindakan perawatan yang efektif tanpa perlu kehadiran fisik pasien di lokasi medis.
 5. Efisiensi Operasional: Dalam lingkungan rumah sakit dan fasilitas kesehatan, IoT dapat digunakan untuk mengoptimalkan pengelolaan aset, inventaris, dan infrastruktur. Hal ini dapat mengurangi biaya operasional dan meningkatkan efisiensi pelayanan.
 6. Penelitian Medis dan Inovasi: Pengumpulan data medis melalui IoT dapat memberikan wawasan berharga bagi penelitian medis dan pengembangan teknologi kesehatan baru. Ini dapat mempercepat penemuan dalam berbagai bidang seperti pengobatan personalisasi, genetika, dan pengembangan obat.
 7. Keamanan dan Kualitas Pasien: IoT dapat membantu memastikan keamanan pasien di lingkungan perawatan, dengan memantau aktivitas pasien dan memberikan peringatan saat terjadi situasi darurat atau risiko jatuh.

7.2 Internet of Things dalam Kesehatan

Dalam bidang kesehatan, IoT menjadi salah satu aplikasi yang terkenal dan populer dengan tujuan memantau tanda-tanda vital pasien secara terus-menerus, sehingga mengurangi

kebutuhan pasien untuk dirawat di rumah sakit. Meskipun sistem kesehatan elektronik (*e-health*) sudah ada sebelum munculnya IoT, dalam aplikasi kesehatan konvensional, komunikasi dua arah antara sensor dan server jarak jauh tidak dapat dilakukan, dan sebuah gateway/server jarak jauh tidak bisa langsung berkomunikasi dengan node sensor. IoT mengubah hal ini dengan memanfaatkan protokol Internet yang sudah ada seperti IPv6, yang memungkinkan alamat langsung diberikan pada berbagai perangkat dan sensor melalui Internet. Jejaring sosial memiliki manfaat yang luas dan memainkan peran penting dalam berbagi informasi dan transfer pengetahuan di berbagai bidang. Dalam mengelola penyakit kronis seperti diabetes, jejaring sosial dapat digunakan untuk meningkatkan kesadaran akan berbagai aspek perilaku sehat seperti pola makan dan olahraga, serta pengetahuan tentang pengelolaan diri. Individu dapat mendapatkan pendidikan dan tingkat kesadaran mereka dapat ditingkatkan melalui berbagi informasi dan diskusi melalui aplikasi jejaring sosial di ponsel yang sangat praktis dan mudah digunakan. Internet of Things Sosial merupakan ekstensi dari Internet of Things, yang memiliki potensi besar untuk berbagai aplikasi. Meskipun belum memiliki kecerdasan yang memadai dan tidak dapat memenuhi tuntutan kinerja aplikasi yang semakin meningkat dari berbagai bidang, teknologi agen tampaknya menjadi pendekatan yang menjanjikan dalam implementasi *Internet of Things Sosial* (Hassanien *et al.*, 2019).

Dalam sistem kesehatan, berbagai sensor diterapkan untuk memantau tanda-tanda vital pasien, termasuk sensor pemantau lingkungan, dan ini cenderung tidak nyaman bagi pasien dan mahal. Ada dua cara untuk mendeteksi dan memprediksi status kesehatan pasien: dengan atau tanpa metode pengenalan aktivitas. Metode non-aktivitas dapat dikelompokkan lebih lanjut menjadi dua kelompok, yaitu metode konvensional dan berbasis IoT.

Metode konvensional mengacu pada pendekatan tradisional dalam mendeteksi dan memprediksi status kesehatan

pasien. Dalam metode ini, data kesehatan pasien disimpan dan dianalisis menggunakan berbagai metode pembelajaran mesin seperti Jaringan Saraf Tiruan (ANN) atau logika fuzzy. Hasil analisis ini digunakan untuk mendeteksi faktor-faktor yang paling signifikan dalam penyakit atau kondisi kesehatan pasien.

Di sisi lain, metode berbasis IoT (*Internet of Things*) melibatkan penggunaan teknologi IoT dalam mengumpulkan dan menganalisis data kesehatan pasien. Dalam pendekatan ini, berbagai sensor yang ditempatkan pada pasien atau lingkungannya mengumpulkan data secara terus-menerus, termasuk tanda-tanda vital, aktivitas, dan lingkungan. Data ini kemudian dikirimkan melalui jaringan dan dianalisis untuk mendeteksi pola atau perubahan yang mungkin mengindikasikan status kesehatan yang abnormal.

Dengan demikian, metode konvensional berfokus pada analisis data historis menggunakan metode pembelajaran mesin, sementara metode berbasis IoT mengandalkan sensor dan teknologi terkoneksi untuk mendapatkan data secara real-time dan mengidentifikasi perubahan dalam status kesehatan pasien secara lebih dinamis.

Metode berbasis IoT memiliki keunggulan dalam menghasilkan data yang lebih akurat dan real-time karena penggunaan sensor yang terus-menerus mengumpulkan informasi langsung dari pasien dan lingkungannya. Selain itu, dengan metode berbasis IoT, komunikasi dua arah antara sensor dan server jarak jauh dapat terjadi, memungkinkan pengiriman data secara langsung untuk analisis lebih lanjut atau tindakan respons yang cepat.

Namun, walaupun metode berbasis IoT memiliki potensi yang kuat untuk mendukung pemantauan kesehatan yang lebih baik dan respons yang lebih cepat, tantangan-tantangan seperti keamanan data, privasi pasien, dan kompleksitas infrastruktur teknologi perlu diatasi dengan cermat. Pengembangan sistem berbasis IoT dalam kesehatan juga memerlukan investasi dalam

perangkat keras, perangkat lunak, dan sumber daya manusia yang terampil.

Kesimpulannya, baik metode konvensional maupun berbasis IoT memiliki peranan penting dalam perkembangan sistem pemantauan kesehatan. Metode konvensional mengandalkan analisis data historis dengan metode pembelajaran mesin, sementara metode berbasis IoT memanfaatkan sensor dan teknologi internet untuk mengumpulkan data secara real-time dan mendukung pemantauan yang lebih dinamis dan responsif terhadap perubahan status kesehatan pasien.

7.3 Tantangan dan Solusi Penggunaan Internet of Things dalam Kesehatan dan Medis

Tantangan Penggunaan *Internet of Things* (IoT) dalam Kesehatan dan Medis:

1. Keamanan dan Privasi Data: Pengumpulan, penyimpanan, dan pengiriman data kesehatan sensitif melalui jaringan dapat menghadirkan risiko keamanan dan pelanggaran privasi yang serius. Informasi pribadi pasien harus dijaga dengan sangat baik agar tidak jatuh ke tangan yang salah.
2. Keterbatasan Interoperabilitas: Berbagai perangkat dan sistem kesehatan yang terkoneksi mungkin berasal dari produsen yang berbeda dengan standar komunikasi yang berbeda-beda. Ini dapat menyulitkan pertukaran data dan integrasi sistem.
3. Ketidakpastian Regulasi: Lingkungan regulasi yang kompleks dan berubah-ubah dalam penggunaan data medis dan teknologi IoT dapat menjadi tantangan. Pengembang dan penyedia layanan harus mematuhi pedoman dan peraturan yang berlaku.
4. Ketersediaan Infrastruktur: Sistem IoT memerlukan infrastruktur jaringan yang andal dan kuat untuk mengirim dan menerima data dengan cepat dan akurat. Di daerah yang

kurang berkembang, ketersediaan infrastruktur mungkin menjadi masalah.

Solusi untuk Penggunaan IoT dalam Kesehatan dan Medis:

1. Enkripsi dan Keamanan Data: Penggunaan enkripsi yang kuat dan metode keamanan canggih dapat melindungi data kesehatan dari akses yang tidak sah. Teknologi blockchain juga dapat digunakan untuk memastikan integritas dan keaslian data.
2. Standar Interoperabilitas: Industri perlu bekerja sama untuk mengembangkan standar komunikasi yang umum untuk perangkat kesehatan dan sistem IoT. Hal ini akan memfasilitasi pertukaran data yang lancar antara berbagai sistem.
3. Kepatuhan Regulasi: Pengembang dan penyedia layanan harus memahami dan mematuhi pedoman dan regulasi yang berlaku dalam pengumpulan dan pengelolaan data medis. Mereka perlu bekerja sama dengan lembaga regulasi dan ahli hukum untuk memastikan kepatuhan.
4. Infrastruktur Jaringan yang Kuat: Investasi dalam infrastruktur jaringan yang kuat dan luas akan mendukung penggunaan IoT dalam kesehatan. Peningkatan konektivitas dan cakupan jaringan akan memastikan data dapat ditransmisikan dengan efisien.
5. Pengembangan Aplikasi yang User-Friendly: Pengembang harus merancang aplikasi dan antarmuka yang mudah digunakan oleh pasien dan profesional kesehatan. Ini akan meningkatkan adopsi teknologi dan penggunaan yang efektif.
6. Pelatihan dan Pendidikan: Profesional kesehatan dan pasien perlu diberikan pelatihan tentang penggunaan dan manfaat teknologi IoT dalam perawatan kesehatan. Pendidikan ini akan membantu meningkatkan pemahaman dan penerimaan terhadap teknologi baru.
7. Pengembangan Model Prediktif: Pemanfaatan analisis data dan kecerdasan buatan untuk mengembangkan model prediktif

dapat membantu mendeteksi dini kondisi abnormal atau risiko kesehatan, sehingga tindakan dapat diambil sebelum menjadi lebih parah.

8. Kemitraan Industri: Kolaborasi antara industri teknologi, penyedia layanan kesehatan, dan pemerintah dapat memfasilitasi pengembangan dan implementasi solusi IoT yang inovatif dan efektif dalam sektor kesehatan.
9. Pengembangan Sensor yang Tepat: Desain dan pengembangan sensor yang akurat, dapat diandalkan, dan nyaman untuk digunakan oleh pasien akan meningkatkan kualitas data yang dikumpulkan dan kenyamanan pasien dalam memantau kesehatan mereka.

Dengan mengatasi tantangan-tantangan ini dan menerapkan solusi yang tepat, penggunaan IoT dalam kesehatan dan medis dapat membawa manfaat besar dalam pemantauan kesehatan pasien, diagnosis yang lebih cepat, perawatan yang lebih efektif, dan peningkatan kualitas hidup.

7.4 Permintaan dan Tantangan Keamanan untuk Beberapa Aplikasi IoT

Seiring dengan kemajuan teknologi dan integrasi IoT (*Internet of Things*) dalam berbagai aspek kehidupan, permintaan dan tantangan keamanan telah menjadi fokus utama dalam penerapan aplikasi IoT. Dalam bagian ini, kita akan mengulas berbagai permintaan serta tantangan yang muncul dalam konteks keamanan untuk beberapa aplikasi khusus dari IoT. Setiap aplikasi memiliki persyaratan keamanan yang unik yang perlu diatasi guna memastikan data, sistem, dan pengguna tetap aman dan terlindungi.

Dalam era yang semakin terhubung ini, IoT telah memperluas batas kemungkinan dalam banyak bidang, termasuk rumah pintar, transportasi, manufaktur, kota cerdas, dan juga

perawatan kesehatan. Meskipun memberikan manfaat besar, integrasi yang mendalam antara perangkat, sensor, dan jaringan juga membawa tantangan baru dalam hal keamanan. Permintaan untuk menjaga integritas, kerahasiaan, dan ketersediaan data menjadi semakin penting, sementara tantangan keamanan yang kompleks juga perlu dihadapi.

Dalam bagian ini, kita akan mengeksplorasi beberapa aplikasi khusus dari IoT, termasuk kesehatan dan medis, serta mengidentifikasi permintaan dan tantangan yang khusus terkait keamanan. Dari pengelolaan data pribadi pasien hingga pengamanan perangkat medis terhubung, akan dianalisis bagaimana permintaan keamanan yang khusus pada setiap aplikasi tersebut menghadirkan tantangan yang kompleks.

Beberapa permintaan dan tantangan keamanan untuk beberapa aplikasi IoT:

1. Rumah Pintar (*Smart Home*):
 - a. Permintaan: Penggunaan IoT dalam rumah pintar memungkinkan pengendalian jarak jauh untuk perangkat seperti lampu, kunci pintu, sistem keamanan, dan termostat. Ini meningkatkan kenyamanan dan efisiensi energi.
 - b. Tantangan: Risiko keamanan datang dari potensi peretasan atau akses yang tidak sah ke sistem rumah pintar. Kehilangan privasi dan penyalahgunaan data pribadi juga menjadi perhatian, terutama jika data rumah tangga dikumpulkan dan disimpan secara online.
2. Kendaraan Terhubung (*Connected Vehicles*):
 - a. Permintaan: Aplikasi IoT dalam kendaraan terhubung dapat meningkatkan keselamatan dengan berbagi informasi lalu lintas dan mencegah kecelakaan melalui sistem pengereman otomatis.
 - b. Tantangan: Keamanan kendaraan dapat terancam oleh peretasan yang dapat memengaruhi sistem navigasi atau

mengambil alih kendali kendaraan. Perlindungan data pribadi dan privasi pengemudi juga perlu diatasi.

3. Manufaktur Cerdas (*Smart Manufacturing*):
 - a. Permintaan: IoT digunakan untuk mengumpulkan data produksi secara real-time, memantau peralatan, dan meningkatkan efisiensi rantai pasok.
 - b. Tantangan: Serangan siber terhadap infrastruktur manufaktur dapat menyebabkan gangguan produksi, dan risiko bocornya rahasia dagang atau desain produk juga perlu diatasi.
4. Kota Cerdas (*Smart Cities*):
 - a. Permintaan: Aplikasi IoT dalam kota cerdas mencakup pemantauan lalu lintas, manajemen limbah, penerangan jalan, dan layanan publik yang lebih baik.
 - b. Tantangan: Keamanan kota cerdas menghadapi risiko serangan siber yang dapat mengganggu layanan kunci seperti listrik, transportasi, atau air bersih. Perlindungan data pengguna juga penting dalam sistem kota cerdas.
5. Kesehatan dan Medis:
 - a. Permintaan: Penggunaan IoT dalam perawatan kesehatan memungkinkan pemantauan pasien secara real-time, diagnosis yang lebih cepat, dan perawatan jarak jauh.
 - b. Tantangan: Keamanan data medis sangat penting untuk mencegah akses yang tidak sah ke informasi pasien. Integritas data dan privasi pasien juga perlu dijaga agar data kesehatan tidak disalahgunakan.

Sedangkan tantangan keamanan khusus dalam aplikasi IoT di bidang kesehatan:

1. Kerahasiaan Data Pasien: Data medis pribadi yang dikumpulkan oleh perangkat IoT harus dienkripsi dan diamankan agar tidak jatuh ke tangan yang salah. Pelanggaran privasi pasien dapat mengakibatkan penyalahgunaan informasi sensitif.

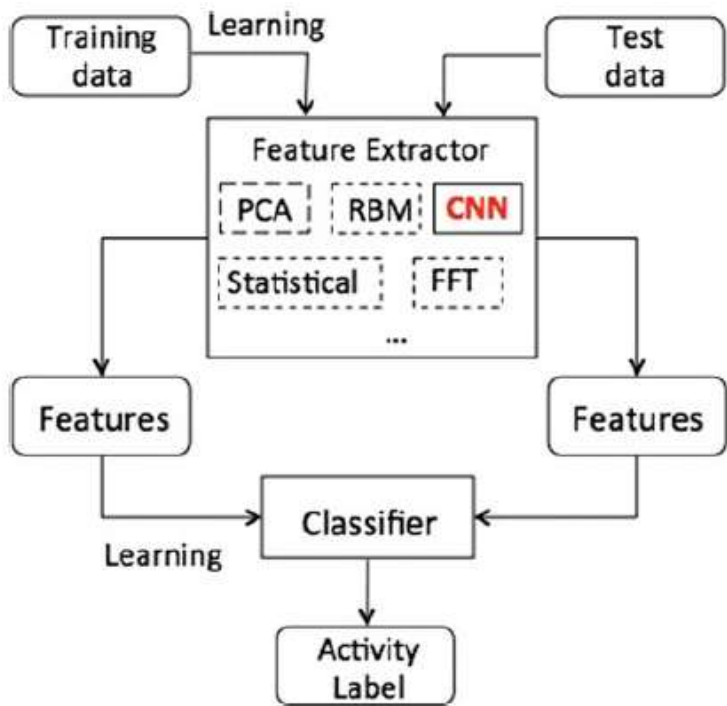
2. **Integritas Data:** Data kesehatan yang dikirim dan diterima oleh perangkat IoT harus dipastikan kebenarannya agar tidak terjadi manipulasi atau perubahan yang dapat menyebabkan diagnosis atau perawatan yang tidak akurat.
3. **Kehandalan Sistem:** Dalam bidang kesehatan, ketepatan dan ketersediaan data sangat penting. Kerentanan pada perangkat atau jaringan dapat berdampak serius pada keamanan dan keselamatan pasien.
4. **Serangan Siber pada Perangkat Medis:** Perangkat medis yang terhubung seperti alat pacu jantung atau pompa insulin rentan terhadap serangan siber yang dapat mengganggu fungsi atau mengambil alih kontrol perangkat.
5. **Regulasi dan Kepatuhan:** IoT dalam kesehatan harus mematuhi peraturan ketat seperti HIPAA (*Health Insurance Portability and Accountability Act*) untuk melindungi privasi dan keamanan data pasien.
6. **Kebocoran Data Medis:** Data medis yang tersimpan dalam perangkat atau di cloud dapat terkena risiko kebocoran jika tidak dilindungi dengan baik. Pengamanan data dan infrastruktur harus menjadi prioritas.

Mengatasi tantangan keamanan ini memerlukan pendekatan holistik yang melibatkan enkripsi kuat, pengembangan perangkat keras dan perangkat lunak yang aman, serta kepatuhan terhadap regulasi industri. Peningkatan kesadaran dan pendidikan tentang keamanan siber juga penting bagi para profesional kesehatan dan pengguna akhir.

7.5 Contoh Metodologi dalam IoT di bidang Kesehatan

Dalam waktu belakangan, Jaringan Saraf Tiruan (*Artificial Neural Networks* - ANNs) memainkan peran yang signifikan dalam aplikasi SIoT (*Social Internet of Things*), terutama pada sensor

medis terbenam. Selain itu, ANNs memunculkan tantangan baru dalam pengembangan dan aplikasi seluler. Para peneliti dalam beberapa penelitian telah memperkenalkan penggunaan SIoT, seperti yang terlihat dalam karya Zeng dkk (Zeng *et al.*, 2015). Dalam karyanya, para peneliti menjelaskan bagaimana sensor terbenam mampu mengenali aktivitas manusia serta memahami perilaku manusia. Mereka memperkenalkan salah satu jenis ANNs yang dikenal sebagai *Convolution Neural Network* (CNN). Dengan tekad untuk mengekstraksi fitur-fitur yang membedakan untuk pengenalan aktivitas, para peneliti ini mengimplementasikan berbagai aspek berdasarkan CNN, termasuk dependensi lokal dan invarian skala dari sinyal ucapan. Upaya peningkatan sistem dilakukan melalui pemanfaatan aplikasi seluler, yang menghasilkan pencapaian akurasi yang tinggi dengan memanfaatkan CNN, sebagaimana terlihat dalam Gambar 7.1.



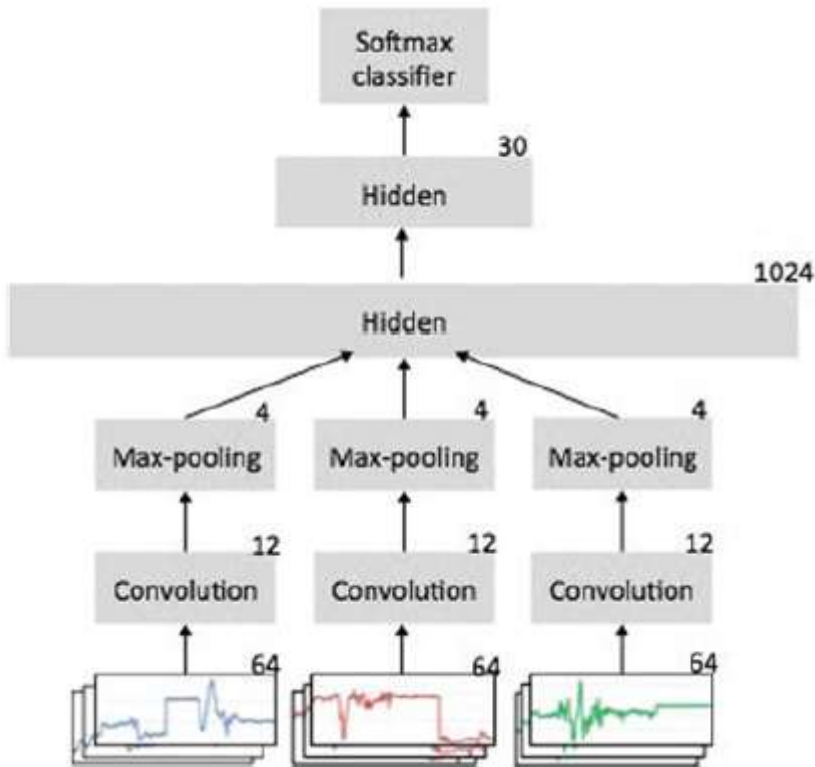
Gambar 7.1. Sistem Pengenalan Aktivitas
Sumber: (Zeng et al., 2015)

Langkah-langkah utama yang dijalankan dalam karya ini meliputi:

1. Ekstraksi fitur berdasarkan prinsip analisis komponen.
2. Penerapan pembelajaran mendalam untuk pengenalan fitur.
3. Pemanfaatan CNN untuk mengklasifikasikan perilaku.

Struktur masukan data melibatkan 64 lapisan, dengan keluaran konvolusi memiliki dimensi 12 dan nilai pooling maksimum sebesar 4. Di sisi lain, sistem ini terdiri dari dua lapisan tersembunyi dengan dimensi 1024 dan 30 (dengan lapisan klasifikasi SOFTMAX sebagai lapisan teratas), seperti yang terlihat

dalam Gambar 7.2. Pendekatan ini berhasil mencapai tingkat akurasi hingga 100%.



Gambar 7.2. CNN untuk pengenalan aktivitas manusia
Sumber: (Zeng *et al.*, 2015)

Banyak peneliti telah mengenalkan metode lain berdasarkan SIoT dan bagaimana penerapannya dalam prediksi dan pengaturan aspek sosial, seperti kunjungan pasien di rumah sakit dan sistem klinis (Chang & Chang, 2018). Dalam penelitian tersebut, para peneliti memperkenalkan kerangka kerja untuk penjadwalan janji rawat jalan (*Outpatients Appointment Scheduling*

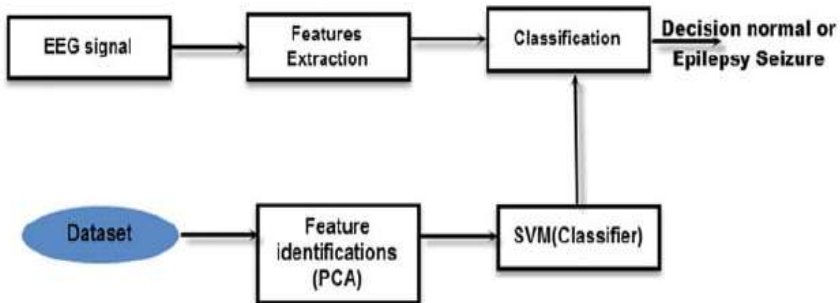
- OAS) di sebuah klinik gigi. Mereka mengenalkan sistem OAS yang berdasarkan beberapa langkah utama sebagai berikut:

1. Memprediksi durasi perawatan menggunakan metode propagasi balik—ANN.
2. Melakukan simulasi operasi klinik gigi berdasarkan simulasi peristiwa diskrit.
3. Melakukan simulasi kinerja penjadwalan janji.

Sistem dalam penelitian ini melayani pasien dan dokter gigi dengan alasan berikut:

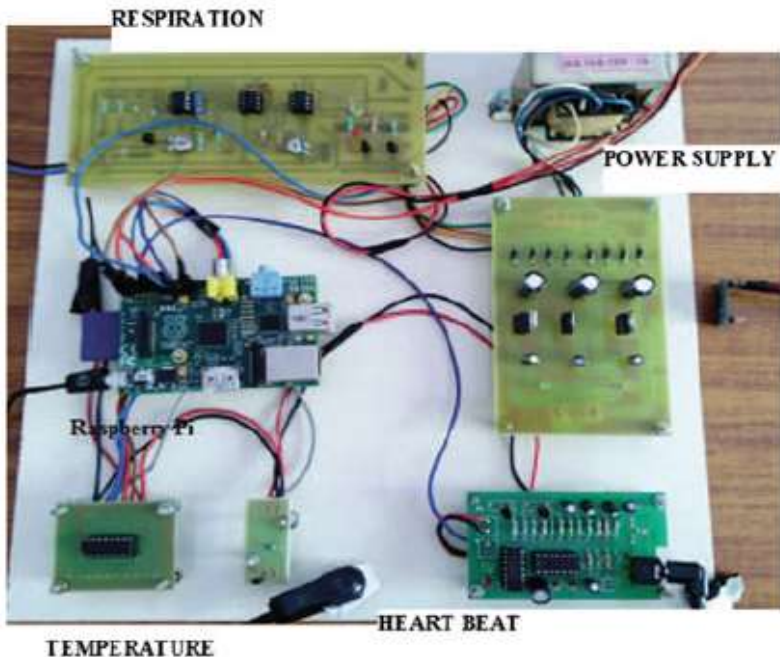
1. Penyedia layanan terdiri dari dokter gigi profesional.
2. Sistem memperkenalkan beragam jenis perawatan medis.

Di sisi lain, metode Mesin Vector Dukungan (*Support Vector Machine* - SVM) telah diperkenalkan dalam berbagai penelitian sebagai salah satu metode klasifikasi yang sangat praktis dalam aplikasi perawatan kesehatan IoT. Dalam buku (Hassanien *et al.*, 2019), para peneliti menerapkan SVM dengan teknik spline untuk mendeteksi tingkat *Epilepsy Seizure* (ES). Sebenarnya, metode SVM dalam penggunaan IoT telah mencapai kinerja yang tinggi. Sensor IoT untuk otak membantu mendeteksi sinyal otak dan mengklasifikasikan ES dengan memanfaatkan SVM. Gambar 7.3 menunjukkan diagram blok dari sistem tersebut. Dataset dikumpulkan dari domain publik dan digunakan dalam sistem, dan penerapan SIoT data online mencapai tingkat akurasi yang tinggi.



Gambar 7.3. Diagram blok sistem deteksi kejang epilepsi
 Sumber: (Hassanien *et al.*, 2019)

SIoT juga membantu dalam analisis big data, terutama data sosial dan publik. Penggunaan sensor detak jantung melalui aplikasi seluler juga membantu meningkatkan sistem diagnosis. Dalam penelitian lain (Kumar & Rajasekaran, 2016), para peneliti menerapkan sensor medis IoT menggunakan kit Raspberry Pi untuk memantau suhu tubuh dan gerakan pasien. Kit Raspberry Pi dengan sensor tersebut terdiri dari beberapa jenis sensor, termasuk pernapasan, detak jantung, dan suhu tubuh, sebagaimana terlihat pada Gambar 7.4.



Gambar 7.4. Monitoring pasien menggunakan Raspberry Pi kit
Sumber: (Hassanien et al., 2019)

Selain itu, dalam penelitian Gupta dkk. (Gupta *et al.*, 2016), para peneliti memperkenalkan desain kit kesehatan cerdas IoT berbasis kit INTEL GALILEO generasi ke-2. Mereka mengumpulkan sejumlah sensor darurat yang memiliki berbagai fitur untuk membantu pasien mengurangi kunjungan ke klinik dengan memantau tekanan darah dan detak jantung, sehingga pasien dapat dibantu sebanyak mungkin tanpa harus selalu pergi ke dokter.

7.6 Metodologi dalam IoT di bidang Kesehatan

Metodologi dalam penerapan *Internet of Things* (IoT) di bidang kesehatan merupakan serangkaian langkah strategis yang dirancang untuk mengintegrasikan teknologi IoT dengan sistem

kesehatan guna meningkatkan pelayanan medis dan pemantauan pasien. Tahapan awal melibatkan identifikasi kebutuhan spesifik dalam konteks kesehatan yang dapat diatasi dengan bantuan IoT. Setelah itu, langkah pemilihan sensor dan perangkat IoT yang sesuai menjadi penting untuk mengumpulkan data medis seperti detak jantung, suhu tubuh, dan tekanan darah. Data tersebut kemudian dikirim melalui jaringan IoT ke platform penyimpanan data yang aman.

Proses selanjutnya melibatkan analisis mendalam terhadap data medis yang dikumpulkan, dimana teknik analisis data dan pengolahan citra digunakan untuk mengenali pola serta tren dalam data tersebut. Keamanan data menjadi fokus utama, mengingat karakteristik sensitif data medis, sehingga enkripsi dan perlindungan data harus diterapkan dengan cermat. Keselarasan dan interoperabilitas dengan sistem kesehatan yang ada juga diperhatikan agar penerapan IoT dapat berjalan secara harmonis.

Pengembangan aplikasi berbasis IoT menjadi langkah kunci dalam metodologi ini, yang memungkinkan para dokter dan pasien untuk mengakses data medis dengan mudah dan menerima rekomendasi perawatan yang relevan. Uji coba dan validasi sistem di lingkungan nyata sangat penting untuk memastikan kinerja yang akurat dan efektif. Setelah itu, integrasi hasil dari sistem IoT ke dalam praktik medis dan pelatihan pengguna menjadi tahapan berikutnya untuk memastikan penggunaan yang optimal dan pemahaman yang tepat terhadap informasi yang diberikan oleh sistem IoT.

Terus-menerus memantau serta meningkatkan sistem merupakan langkah akhir dalam metodologi ini. Dengan demikian, penerapan IoT di bidang kesehatan dapat berjalan secara efisien, aman, dan memberikan manfaat yang signifikan bagi pasien serta penyedia layanan kesehatan. Melalui pendekatan yang terstruktur ini, IoT memiliki potensi besar untuk mengubah dan meningkatkan cara pelayanan kesehatan dipraktikkan dan diterima.

7.6.1 Diagnosis Jantung berbasis Arduino Kit dan IoT

Sistem ini terdiri dari empat bagian utama seperti yang ditunjukkan pada Gambar 7.5. Bagian pertama adalah sensor detak jantung dengan rangkaian ARDUINO. Bagian ini dianggap salah satu bagian penting karena merupakan hubungan antara pasien dan Laptop. Bagian ini diaplikasikan dalam dua tahap pengujian:

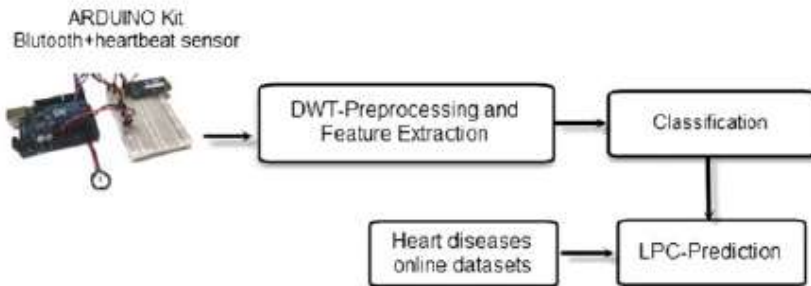
1. Tahap pertama adalah hubungan antara pasien dengan sensor detak jantung, Kit ARDUINO, dan laptop melalui kabel seperti yang ditunjukkan pada Gambar 7.6.
2. Tahap kedua adalah hubungan antara pasien dengan sensor detak jantung, Kit ARDUINO, Bluetooth, dan laptop seperti yang ditunjukkan pada Gambar 7.7.

Sensor merekam detak jantung pasien melalui unit Bluetooth dan dirancang perangkat lunak dalam MATLAB 2017a untuk membaca data real-time dari pasien guna mendiagnosis kondisi pasien dan juga memprediksi komplikasi masa depan seperti yang ditunjukkan pada Gambar 7.8. Bagian kedua dalam diagram blok sistem adalah tahap pra-pemrosesan yang bergantung pada transformasi gelombang diskrit (*Discrete Wavelet Transform* - DWT) untuk menyaring dan meningkatkan sinyal EKG serta mengekstrak fitur-fitur seperti dalam karya Rahouma dkk. (Rahouma & Muhammad, 2017). Alasan penggunaan DWT adalah: (a) Memulihkan sinyal asli dari sinyal berisik. (b) Menganalisis sinyal dalam domain waktu dan frekuensi. (c) Mewakili fungsi dalam kasus memiliki diskontinuitas dan puncak tajam secara lebih efisien daripada hanya menggunakan Transformasi Fourier Diskrit (*Discrete Fourier Transform* - DFT).

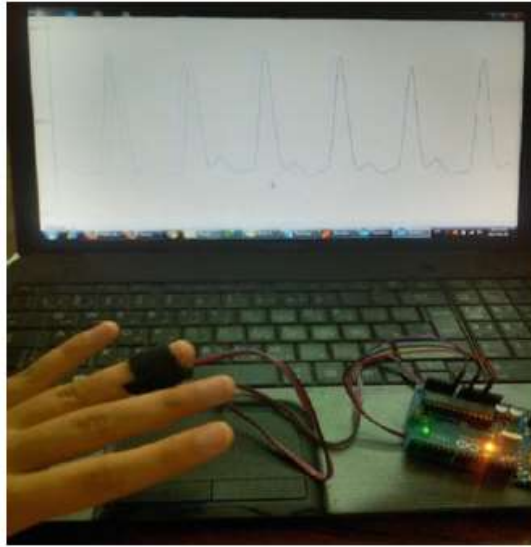
Pemrosesan utama DWT terdiri dari tiga bagian (Rahouma & Muhammad, 2017):

1. Proses dekomposisi.
2. Penyambungan ambang.
3. Proses rekonstruksi.

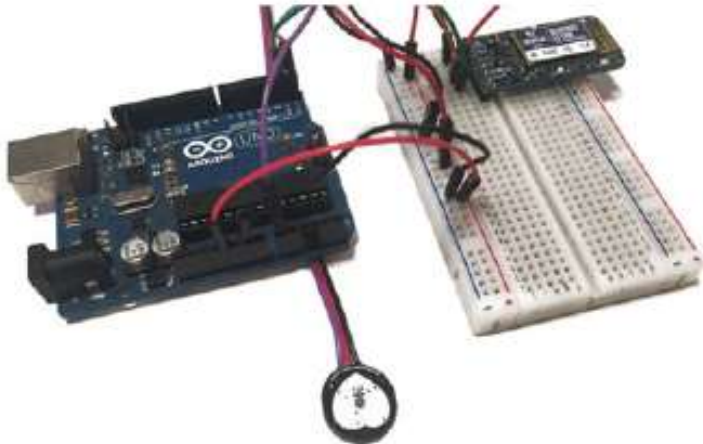
Setelah menerapkan pemrosesan utama DWT, akan diekstrak fitur-fitur dan mendeteksi fitur-fitur utama (RR, QRS, ST, QT, PR). Fitur-fitur normal yang digunakan dalam proses diagnosis tercantum dalam Tabel 7.1. Basis data online tentang penyakit jantung memainkan peran penting dalam klasifikasi untuk mendiagnosis penyakit pasien. Setelah mengumpulkan fitur-fitur penyakit, akan dibandingkannya dengan fitur-fitur saat ini dari pasien seperti dalam (Rahouma & Muhammad, 2017). Di sisi lain, tahap terakhir dari sistem ini adalah prediksi. Teknik prediksi dianggap salah satu yang paling penting dalam diagnosis dini (Loong *et al.*, 2010). Dalam sistem ini, diterapkan Metode Pemrograman Prediksi Linear (*Linear Prediction Coding* - LPC). Metode ini diperkenalkan dalam karya Rahouma dkk. (Rahouma & Muhammad, 2017) dan telah terbukti memiliki akurasi tinggi hingga 100%.



Gambar 7.5. Monitoring pasien menggunakan Raspberry Pi kit
Sumber: (Hassanien et al., 2019)



Gambar 7.6. Arduino yang terhubung dengan sensor detak jantung. Sumber: (Hassanien et al., 2019)



Gambar 7.7. Arduino yang terhubung dengan sensor detak jantung dan bluetooth
Sumber: (Hassanien et al., 2019)

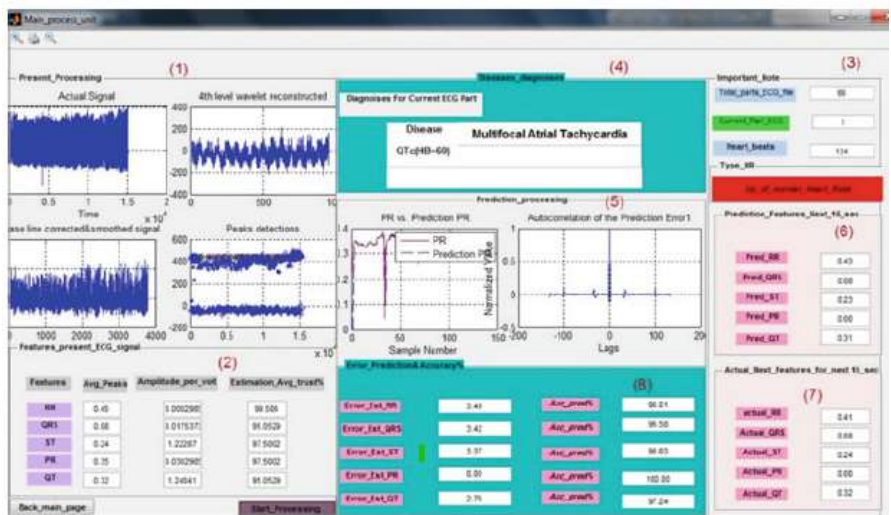
Tabel 7.1. Fitur normal

Name of feature wave	Standard normal value (ms)
RR	0.6–1.2
ST	0.08–0.12
QRS	0.08–0.12
PR	0.12–0.2

Dalam bagian ini, akan disajikan hasil yang diperoleh berdasarkan bagian sebelumnya. Seperti yang telah dibahas sebelumnya, sistem menggunakan MATLAB 2017a dirancang. Strategi sistem akan sebagai berikut:

1. Terapkan kit sensor pada pasien dan baca data secara nirkabel, kemudian kirimkan data tersebut ke laptop atau komputer pribadi (PC) dari server klinik atau rumah sakit, dan juga bisa dikirimkan secara daring berbasis internet.
2. Sistem akan mengambil file data pasien yang disimpan dari server atau laptop dan membaginya menjadi sampel-sampel.
3. Data yang direkam akan dikirimkan atau direkam dalam rentang waktu 1 hingga 10 menit.
4. Seperti dalam Rahouma dkk. (Rahouma & Muhammad, 2017), mereka menggunakan 1.000.000 sampel, dengan frekuensi sampling 250 sampel per detik. Mereka membagi sampel-sampel tersebut menjadi kelompok-kelompok, di mana setiap kelompoknya berkorespondensi dengan rentang waktu 10 menit, sehingga mereka memproses sampel-sampel dari menit pertama (15.000 sampel) dari periode tersebut dan menyimpan hasilnya pada layar untuk 9 menit sisanya. Antarmuka Pengguna (GUI) mencakup semua hasil dalam bentuk nilai dan gambaran, seperti yang ditunjukkan pada Gambar 7.8: (a) Konstruksi DWT adalah proses dekomposisi dan rekonstruksi sinyal. (b) DWT menghasilkan koefisien filter low pass dan high pass. (c) Koefisien estimasi diambil dari koefisien filter lowpass. (d) DWT dianggap sebagai metode

yang sangat baik untuk analisis domain waktu dan frekuensi. (e) Hasil menunjukkan bahwa beberapa nilai tidak normal, yang berarti perlu diterapkannya teknik prediksi untuk memprediksi komplikasi masa depan. (f) Denyut jantung dihitung menggunakan RR sebagai: $60/RR = 133,33$ bpm. (g) LPC mencapai dari 95 hingga 99,9% untuk komplikasi masa depan berdasarkan kumpulan data historis penyakit jantung.

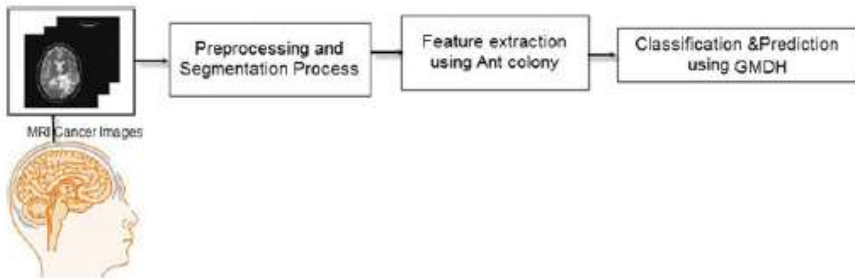


Gambar 7.7. Antarmuka Pengguna (Graphical User Interface - GUI) dari sistem diagnosis sensor detak jantung
Sumber: (Hassanien *et al.*, 2019)

7.6.2 Diagnosis Otak berbasis Sinyal Data Klinis Real Time

Sistem ini terdiri dari tiga bagian utama seperti yang ditunjukkan pada Gambar 7.8 dimana menggunakan teknik computer vision. Tahap utama dari sistem ini mewakili SIoT dalam bentuk kumpulan data online dari peralatan MRI di mana rumah sakit membuat laporan online dengan dataset online dan berbagi dengan klinik dan rumah sakit lainnya. Selain itu, beberapa rumah

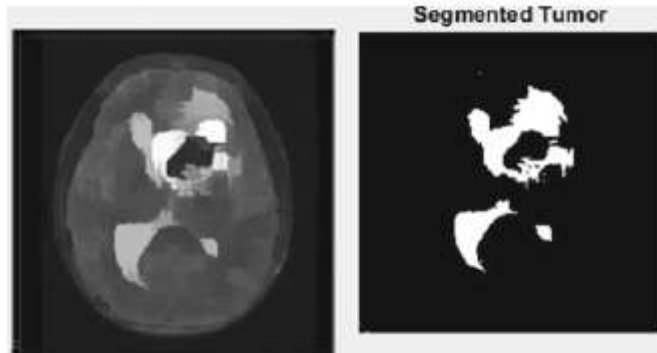
sakit memiliki sistem pemantauan waktu nyata dengan pasien dan mereka menyimpan data di beberapa situs web.



Gambar 7.8. Diagram blok sistem
Sumber: (Hassanien et al., 2019)

- (1) Tahap pra-pemrosesan terdiri dari dua bagian utama:
- Proses filter yang merupakan filter low pass.
 - Proses segmentasi yang mencakup:
 - (a) Analisis thresholding dan binarisasi setelah peningkatan.
 - (b) Proses segmentasi berdasarkan kluster K-means.
Kluster K-means telah diterapkan untuk membagi tumornya dari gambar MRI. Segmentasi akan membantu dalam ekstraksi fitur dan klasifikasi derajat tumor. Algoritma k-means membagi satu set data menjadi K kelompok dari kluster yang saling berbeda seperti dalam proses pengelompokan. Metode yang digunakan untuk menghitung jarak data pusat adalah "jarak Euclidean" (Zeinalkhani et al., 2018).
 - (c) Berdasarkan jarak (d) dan atribut semua piksel yang diperoleh, hitung ulang posisi baru pusat berdasarkan Persamaan (4).

- (d) Ulangi proses tersebut sampai memenuhi kesalahan minimum.
- (e) Ekstrak segmentasi dari gambar MRI seperti yang ditunjukkan pada Gambar 7.9.



Gambar 7.9. K-means clustering untuk segmentasi tumor otak
Sumber: (Hassanien et al., 2019)

- (2) Ekstraksi fitur berdasarkan Optimisasi Koloni Semut (*Ant Colony Optimization* - ACO): Dalam optimisasi koloni semut, komunikasi tidak langsung yang digunakan disebut feromon. Jumlah feromon didasarkan pada jarak, kualitas, dan jumlah sumber makanan. Algoritma koloni semut buatan diperkenalkan dalam [8]. Para penulis telah memperkenalkan solusi masalah optimisasi koloni semut dan kemudian menerapkannya untuk memecahkan masalah salesman keliling. Tujuan dari optimisasi koloni semut adalah untuk menemukan jalur terpendek ke makanan semut dan salesman keliling mencapainya dengan waktu dan jalur terpendek. Dalam penelitian ini, di optimisasi koloni semut berdasarkan salesman keliling untuk metode ekstraksi dan pemilihan fitur untuk gambar MRI biner dari berbagai kasus tumor otak (Wu *et al.*, 2019). Algoritma untuk Koloni Semut didasarkan pada salesman

keliling (ACO-TSP) dan komunikasi tidak langsung feromon.

(3) Metode Klasifikasi dan Prediksi GMDH:

Metode pengelolaan data kelompok (*Group Method of Data Handling* - GMDH) digunakan untuk klasifikasi dan prediksi fitur-fitur yang diprediksi dari basis data tumor otak MRI. GMDH memiliki struktur yang sama dengan Jaringan Saraf Tiruan Polinomial (*Polynomial Neural Network* - PNN). PNN adalah metode paling praktis sebagai jenis Jaringan Saraf Tiruan (*Artificial Neural Network* - ANN). Selain itu, GMDH adalah jaringan multilayer yang menggunakan neuron kuadratik yang menawarkan solusi efektif untuk pemodelan sistem non-linear.

Hasil dan Diskusi Metode Diagnosis Tumor SloT Sistem dalam beberapa penelitian ini didasarkan pada klasifikasi dan prediksi gambar tumor otak. filter low pass diterapkan untuk meningkatkan gambar tumor otak. Selanjutnya, setelah proses thresholding dan proses binarization, diterapkan metode K-means untuk proses segmentasi. Proses ekstraksi fitur didasarkan pada segmentasi optimal tumor yang membantu dalam proses klasifikasi dan prediksi.

Koloni semut berdasarkan salesman keliling (ACO-TSP) mencapai solusi terbaik dalam proses klasifikasi dan prediksi. Dalam ACO-TSP, model matriks dibuat berdasarkan data yang telah tersegmentasi dan setelah itu digunakan analisis komponen utama (*Principal Component Analysis* - PCA) untuk mengekstraksi fitur umum optimal dari gambar yang telah tersegmentasi dan setelah itu dihitunglah 7 fitur dari 100 fitur umum berdasarkan persamaan yang ada dalam Tabel 7.2 dan batas maksimum iterasi adalah 500. Model ACO-TSP membantu menghemat waktu di CPU (Gülcü *et al.*, 2016). Selain itu, algoritma ACO-TSP diterapkan untuk ekstraksi fitur pada sistem laptop yang sama. Hasilnya menunjukkan bahwa semua fitur dari setiap gambar membutuhkan waktu 5 menit

untuk seluruh proses termasuk semua tahap (preprocessing, segmentasi, ekstraksi fitur, klasifikasi, dan prediksi), yang berarti untuk semua tahap. Dengan menerapkan alat pemrosesan paralel MATLAB pada sistem laptop, didapatkan waktu total 2 menit untuk semua fitur. Akurasi penggunaan ACO-TSP setelah klasifikasi dan prediksi berkisar dari 95% hingga 99,8%.

Tabel 7.2. Persamaan untuk untuk ekstraksi fitur (ACO)

Name of equations	Equation
Mean	$\mu = \frac{\sum x}{N}$
Standard deviation	$\sigma = \sqrt{\frac{1}{N} \sum_{i=1}^N (x_i - \mu)^2}$
Entropy	$ENT = - \sum_i \sum_j x(i, j) \log_2 x(i, j)$
Root mean square (RMS)	$RMS = \frac{1}{N} \sum_{i=1}^N x^2(i)$
Variance	$\sigma^2 = \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} (i - \mu)^2 x(i, j)$
Smoothness	$Smoothness = 1 - \left(\frac{1}{(1+\sigma^2)} \right)$
Kurtosis	$Ku = \frac{1}{\sigma^4} \sum_{i=0}^{m-1} (i - \mu)^4 x(i) - 3$

DAFTAR PUSTAKA

- Chang, W.-J., & Chang, Y.-H. 2018. Design of a Patient-Centered Appointment Scheduling with Artificial Neural Network and Discrete Event Simulation. *Journal of Service Science and Management*, 11(01), 71–82. <https://doi.org/10.4236/jssm.2018.111007>
- Gülcü, Ş., Mahi, M., Baykan, Ö. K., & Kodaz, H. 2016. A parallel cooperative hybrid method based on ant colony optimization and 3-Opt algorithm for solving traveling salesman problem. *Soft Computing*, 1669–1685.
- Gupta, P., Agrawal, D., Chhabra, J., & Dhir, P. K. 2016. IoT based smart healthcare kit. *2016 International Conference on Computational Techniques in Information and Communication Technologies, ICCTICT 2016 - Proceedings, March*, 237–242. <https://doi.org/10.1109/ICCTICT.2016.7514585>
- Hassanien, A. E., Bhatnagar, R., Khalifa, N. E. M., & Taha, M. H. N. 2019. Toward Social Internet of Things (SIoT); Enabling Technologies, Architectures and Applications. In *Studies in Computational Intelligence* (Vol. 846). Springer. https://doi.org/10.1007/978-3-030-24513-9_8
- Kumar, R., & Rajasekaran, M. P. 2016. An IoT based patient monitoring system using raspberry Pi. *2016 International Conference on Computing Technologies and Intelligent Data Engineering (ICCTIDE'16)*, 1–4. <https://doi.org/10.1109/ICCTIDE.2016.7725378>
- Loong, J. L. C., Subari, K. S., Besar, R., & Abdullah, M. K. 2010. A new approach to ECG biometric systems: a comparative study between LPC and WPD systems. *International Scholarly and Scientific Research & Innovation*, 4(8), 340–345. <https://waset.org/journals/waset/v44/v44-123.pdf>

- Ortiz, A. M., Hussein, D., Park, S., Han, S. N., & Crespi, N. 2014. The Cluster Between Internet of Things and Social Networks: Review and Research Challenges. *IEEE Internet of Things Journal*, 1(3), 206–215. <https://doi.org/10.1109/IJOT.2014.2318835>
- Rahouma, K. H., & Muhammad, R. H. 2017. *Heart Diseases Detection Based on Analysis and Diagnosis of Heart Diseases Detection Based on Analysis and Diagnosis of Electrocardiogram Using Wavelet Transform and Prediction of Future Complications*. November, 10–30. <https://doi.org/10.13141/RG.2.2.35948.41608>
- Wu, Y., Gong, M., Ma, W., & Wang, S. 2019. High-order graph matching based on ant colony optimization. *Neurocomputing*, 328, 97–104.
- Zeinalkhani, L., Ali Jamaat, A., & Rostami, K. 2018. Diagnosis of Brain Tumor Using Combination of K-Means Clustering and Genetic Algorithm. *Iranian Journal of Medical Informatics*, 7(1), 6. <https://doi.org/10.24200/ijmi.v7i0.159>
- Zeng, M., Nguyen, L. T., Yu, B., Mengshoel, O. J., Zhu, J., Wu, P., & Zhang, J. 2015. Convolutional Neural Networks for human activity recognition using mobile sensors. *Proceedings of the 2014 6th International Conference on Mobile Computing, Applications and Services, MobiCASE 2014, July 2015*, 197–205. <https://doi.org/10.4108/icst.mobicase.2014.257786>

BAB 8

KEAMANAN DAN PRIVASI DALAM INTERNET OF THINGS

Oleh Suwito Pomalingo

8.1 Pendahuluan

Era digital telah membawa kita ke dalam dunia di mana segala sesuatu semakin terkoneksi, membentuk jaringan yang dikenal sebagai *Internet of Things* (IoT). Perkembangan teknologi ini tidak hanya merubah cara kita berinteraksi dengan dunia di sekitar kita, namun juga menjanjikan efisiensi dan kemudahan dalam berbagai aspek kehidupan kita. Contohnya saja, saat ini betapa penting untuk melakukan monitoring kualitas udara dengan IoT setelah selama 2 tahun dilanda pandemic Covid 19 (Widjaja, Halim and Andarini, 2022). Namun, di balik potensi luar biasa yang ditawarkan oleh IoT, terdapat tantangan signifikan yang perlu kita hadapi, khususnya dalam aspek keamanan dan privasi.

Keamanan dan privasi menjadi isu penting dalam IoT, mengingat tingginya volume dan jenis data yang dihasilkan dan dikumpulkan oleh perangkat IoT (Halim and Hutagalung, 2022). Selain itu, sifat dari IoT yang terhubung dan terbuka menimbulkan celah yang dapat dimanfaatkan oleh pihak yang tidak bertanggung jawab untuk melakukan serangan dan penyalahgunaan data. Dengan memahami konsep keamanan dan privasi dalam konteks IoT, kita dapat mengambil langkah-langkah proaktif untuk melindungi diri dan komunitas kita dari risiko yang mungkin timbul. Pada sub bab ini, kita akan membahas secara mendalam tentang keamanan dan privasi dalam IoT, mulai dari tantangan, teknologi yang digunakan, hingga solusi masa depan untuk meningkatkan keamanan dan privasi dalam IoT.

8.1.1 Pentingnya Keamanan dan Privasi dalam IoT

Keamanan dan privasi merupakan dua pilar penting dalam operasional dan pengembangan *Internet of Things* (IoT). Menurut sebuah laporan yang diterbitkan oleh Cisco pada tahun 2020, diperkirakan akan ada sekitar 50 miliar perangkat IoT yang terkoneksi ke internet pada tahun 2023 (Cisco, 2020). Ini berarti terdapat volume data yang sangat besar yang dihasilkan. Mengingat luasnya cakupan IoT dan beragam jenis informasi yang ditangani, pemahaman tentang pentingnya keamanan dan privasi menjadi sangat penting. Informasi yang ditangani ini mulai dari data pribadi hingga informasi bisnis yang sangat sensitif. Perlindungan atas data ini menjadi sangat penting, terutama dalam era digital saat ini. Menjaga integritas dan kerahasiaan data ini adalah hal yang sangat penting.

Keamanan dalam IoT bertujuan untuk melindungi perangkat dan jaringan dari berbagai jenis serangan. Serangan ini bisa dalam bentuk yang dapat mengganggu operasional, merusak perangkat, atau mencuri data. Dengan semakin banyaknya jumlah perangkat IoT, titik serangan juga menjadi semakin banyak. Tanpa perlindungan yang tepat, perangkat IoT dapat menjadi sasaran empuk bagi pelaku serangan siber. Sebuah laporan yang diterbitkan oleh Symantec pada tahun 2019 menyebutkan bahwa serangan terhadap perangkat IoT telah meningkat sebesar 600% dalam kurun waktu satu tahun (Symantec, 2019). Perlindungan ini sangat penting agar kita dapat merasakan manfaat dari IoT tanpa harus khawatir dengan ancaman keamanan. Oleh karena itu, keamanan dalam IoT menjadi isu yang sangat penting.

Privasi dalam konteks IoT berkaitan erat dengan perlindungan data pengguna. Data ini adalah data yang dikumpulkan, diproses, dan disimpan oleh perangkat IoT. Setiap perangkat IoT memiliki potensi untuk mengumpulkan data pribadi pengguna, baik secara langsung maupun tidak langsung. Perlindungan atas data pribadi ini bukan hanya menjadi tuntutan hukum, seperti yang diatur dalam *General Data Protection*

Regulation (GDPR) di Uni Eropa. Perlindungan ini juga menjadi harapan dari pengguna itu sendiri. Penelitian yang dilakukan oleh Greenleaf pada tahun 2017 menunjukkan bahwa pengguna mengharapkan adanya perlindungan atas data pribadi mereka (Greenleaf, 2017). Oleh karena itu, privasi dalam konteks IoT menjadi isu yang sangat penting.

Secara keseluruhan, keamanan dan privasi menjadi bagian integral dari IoT. Dengan mengimplementasikan keamanan dan privasi yang baik, kita tidak hanya menjaga kepercayaan pengguna, tetapi juga memastikan bahwa teknologi IoT dapat digunakan dengan cara yang aman dan bertanggung jawab. Dalam konteks transformasi digital, penting bagi kita untuk memahami dan menerapkan konsep keamanan dan privasi dalam IoT. Ini tidak hanya akan membantu kita dalam menjaga kepercayaan pengguna, tetapi juga dalam memastikan bahwa teknologi IoT dapat memberikan manfaat yang optimal. Oleh karenanya, perlu adanya pemahaman yang baik dan aplikasi yang tepat dari konsep keamanan dan privasi dalam IoT.

8.1.2 Konsep Keamanan Dan Privasi Dalam IoT

Konsep keamanan dalam *Internet of Things* (IoT) mencakup beberapa aspek penting, termasuk perlindungan perangkat, perlindungan jaringan, dan perlindungan data. Perlindungan perangkat berfokus pada menjaga integritas fisik dan perangkat lunak dari perangkat IoT, mencegah mereka dari kerusakan atau manipulasi. Perlindungan jaringan berfokus pada pengamanan komunikasi antara perangkat IoT dan infrastruktur pendukungnya, mencegah akses yang tidak sah dan serangan DDoS. Perlindungan data berfokus pada menjaga integritas dan kerahasiaan data yang dikumpulkan dan diproses oleh perangkat IoT. Menurut studi yang diterbitkan oleh Roman, Najera, dan Lopez, perangkat IoT harus dirancang dan dikelola dengan mempertimbangkan semua aspek ini untuk mencapai tingkat keamanan yang memadai (Roman, Najera and Lopez, 2011).

Konsep privasi dalam IoT berkaitan dengan pengumpulan, penggunaan, dan penyimpanan data pengguna. Pengguna memiliki hak untuk mengetahui data apa yang dikumpulkan, bagaimana data tersebut digunakan, dan siapa yang dapat mengakses data tersebut. Hal ini sejalan dengan prinsip "*privacy by design*" yang mengharuskan perusahaan untuk memasukkan fitur-fitur privasi sejak awal perancangan perangkat IoT. Prinsip ini juga termasuk dalam *General Data Protection Regulation* (GDPR) Uni Eropa, yang memandatkan bahwa pengguna harus memiliki kontrol atas data mereka. Menurut studi yang dilakukan oleh Weber (Weber, 2010), memahami dan menerapkan konsep privasi dalam IoT sangat penting untuk memastikan bahwa teknologi ini tidak melanggar hak-hak pengguna.

Untuk mencapai keamanan dan privasi dalam IoT, ada beberapa strategi yang dapat diterapkan. Hal ini dapat mencakup penerapan teknologi enkripsi, otentikasi, dan teknologi lainnya untuk melindungi data dan komunikasi (Ahmad *et al.*, 2018). Di sisi lain, untuk menjaga privasi, penggunaan teknologi seperti anonimisasi dan pemisahan data dapat menjadi solusi yang efektif. Peran dari regulasi dan standar juga sangat penting untuk mendukung upaya ini.

8.2 Ancaman Keamanan dan Privasi dalam IoT

8.2.1 Ancaman Keamanan dalam IoT

Perkembangan *Internet of Things* (IoT) telah merubah cara kita hidup dan bekerja, memberikan kemudahan dalam berbagai aspek kehidupan sehari-hari. Namun, di balik kemudahan yang ditawarkannya, IoT juga membawa berbagai ancaman keamanan yang baru dan lebih kompleks. Penyusup dapat mengeksploitasi kerentanan perangkat lunak dan perangkat keras, meluncurkan serangan terhadap jaringan, atau mencuri data sensitif yang dikumpulkan dan diproses oleh perangkat IoT. Menghadapi tantangan ini, pemahaman mendalam tentang ancaman keamanan

dalam IoT dan bagaimana cara melindunginya menjadi hal yang sangat penting. Berikut beberapa ancaman keamanan dalam IoT yang dikategorikan menjadi tiga, yaitu:

1. *Endpoint Attacks*

Dalam konteks IoT, istilah *endpoint* merujuk pada setiap perangkat yang terhubung ke jaringan, seperti sensor, kamera, dan berbagai perangkat lainnya. Banyak dari perangkat ini dirancang dengan fokus pada fungsi utama, dan sering kali keamanan menjadi pertimbangan sekunder. Oleh karena itu, perangkat-perangkat ini menjadi rentan terhadap berbagai jenis serangan *endpoint*. Serangan ini dapat melibatkan upaya untuk mendapatkan akses yang tidak sah ke perangkat atau jaringan, mencuri data, atau merusak fungsi perangkat. Perangkat IoT menjadi target menarik bagi penyerang karena kerentanan ini. Ini merupakan tantangan besar dalam mewujudkan IoT yang aman dan andal (Roman, Najera and Lopez, 2011).

Serangan endpoint dapat terjadi dalam berbagai bentuk, termasuk serangan melalui malware, ransomware, atau phishing. Sebagai contoh, penyerang dapat mencoba mengeksploitasi kerentanan perangkat lunak untuk menginstal malware pada perangkat IoT. Menurut laporan dari Symantec, perangkat IoT banyak menjadi target serangan malware (Symantec, 2019). Malware tersebut memungkinkan penyerang untuk mengontrol perangkat dan meluncurkan serangan DDoS atau mengumpulkan dan mencuri data pribadi. Di sisi lain, serangan ransomware dapat mengenkripsi data pada perangkat dan menuntut tebusan untuk mendekripsi kembali. Phishing juga bisa digunakan untuk mendapatkan akses ke perangkat melalui pengguna yang tidak curiga. Semua ancaman ini menunjukkan pentingnya perlindungan *endpoint* yang kuat dalam lingkungan IoT.

Membuat *endpoint* menjadi aman adalah tantangan yang kompleks, karena melibatkan berbagai aspek mulai dari perangkat keras, perangkat lunak, hingga manajemen jaringan. Dalam beberapa kasus, *endpoint* yang tidak aman bisa menjadi titik masuk bagi penyerang untuk mendapatkan akses ke jaringan yang lebih luas. Sebagai contoh, jika perangkat IoT di rumah atau perusahaan dikompromikan, penyerang dapat merusak jaringan perangkat, mencuri data, atau melakukan serangan lainnya. Untuk itu, keamanan pada setiap perangkat IoT sangat penting, karena bisa berdampak pada sistem yang lebih luas. Oleh karena itu, strategi keamanan IoT harus mencakup perlindungan *endpoint*, yang memerlukan kombinasi dari keamanan perangkat keras dan perangkat lunak, serta pemantauan dan manajemen jaringan yang tepat. Upaya ini penting untuk mencegah, mendeteksi, dan merespons ancaman secara efektif (Alaba *et al.*, 2017). Mengingat pentingnya isu ini, harus ada lebih banyak penelitian dan pengembangan dalam bidang keamanan IoT, terutama terkait dengan perlindungan *endpoint*.

2. *Network Attacks*

Serangan pada jaringan melibatkan aktivitas berbahaya yang dirancang untuk merusak integritas, ketersediaan, atau kerahasiaan jaringan dan data. Hal ini menjadi masalah serius, karena sistem IoT sering terdiri dari banyak perangkat yang saling terhubung dalam satu jaringan, dan kompromi pada satu perangkat bisa berdampak pada keseluruhan sistem.

Salah satu contoh serangan jaringan dalam IoT adalah serangan *Denial of Service* (DoS) dan *Distributed Denial of Service* (DDoS). Serangan jenis ini bertujuan untuk membuat jaringan atau sistem menjadi tidak tersedia, misalnya dengan membanjiri jaringan dengan lalu lintas yang tidak perlu atau menghabiskan sumber daya sistem

(Sicari *et al.*, 2015). Akibatnya, perangkat atau sistem yang sah tidak dapat mengakses layanan yang mereka butuhkan. Solusi untuk melindungi sistem IoT dari serangan jaringan melibatkan penerapan mekanisme keamanan yang kuat pada tingkat jaringan, termasuk firewall, deteksi intrusi, dan sistem pencegahan, serta enkripsi data yang kuat (Al-Fuqaha *et al.*, 2015). Selain itu, pemantauan jaringan yang kontinu juga penting untuk mendeteksi dan merespons serangan secepat mungkin. Meski tantangannya cukup besar, melindungi jaringan IoT dari serangan ini adalah bagian penting dalam memastikan keandalan dan keamanan IoT.

3. *Physical Attacks*

Selain ancaman yang bersifat digital, *Internet of Things* (IoT) juga rentan terhadap serangan fisik. Serangan fisik ini merujuk pada tindakan yang dilakukan secara langsung terhadap perangkat IoT, seperti pencurian, kerusakan fisik, atau manipulasi perangkat (Mosenia and Jha, 2017). Dalam banyak kasus, perangkat IoT berada di lokasi yang mudah diakses, baik di dalam rumah, di perusahaan, atau di tempat umum, yang membuatnya rentan terhadap serangan ini.

Salah satu contoh serangan fisik adalah *Side Channel Attacks* (SCA), di mana penyerang mengumpulkan informasi dari perangkat dengan melihat konsumsi daya, radiasi elektromagnetik, atau variabel fisik lainnya (Standaert, 2010). Informasi yang diperoleh dari serangan ini bisa digunakan untuk memecahkan sistem keamanan yang ada pada perangkat. Selain itu, perangkat IoT juga bisa jadi target pencurian fisik yang dapat mengakibatkan hilangnya data atau fungsi penting.

Untuk menghadapi serangan fisik, perangkat IoT harus dilengkapi dengan fitur keamanan fisik, seperti perlindungan anti-tamper, kriptografi perangkat keras, dan

mekanisme deteksi intrusi fisik (Bonomi *et al.*, 2012). Namun, penerapan keamanan fisik ini bisa menjadi tantangan, terutama karena keberagaman dan jumlah perangkat IoT yang ada. Upaya perlindungan ini penting untuk memastikan keamanan dan keandalan seluruh ekosistem IoT.

8.2.2 Ancaman Privasi dalam IoT

Tantangan terbesar dalam era *Internet of Things* (IoT) tidak hanya terbatas pada ancaman keamanan, namun juga meliputi isu privasi. Dalam masyarakat yang semakin terkoneksi, sejumlah besar data pribadi dikumpulkan, diproses, dan dikirimkan melalui berbagai perangkat IoT. Meskipun kemajuan teknologi ini membawa banyak kemudahan, potensi pelanggaran privasi pengguna menjadi ancaman yang serius. Konsekuensinya, dapat merusak kepercayaan pengguna dan merintangi adopsi IoT. Oleh karena itu, memahami dan menangani ancaman privasi dalam IoT menjadi aspek krusial dalam upaya mewujudkan transformasi digital yang aman dan terpercaya.

Berikut beberapa ancaman terhadap privasi dalam IoT

1. Penyalahgunaan Data

Salah satu ancaman privasi paling serius dalam Internet of Things (IoT) adalah penyalahgunaan data. Dengan perangkat IoT yang terus mengumpulkan dan mengirimkan data pengguna, ada risiko bahwa informasi pribadi bisa jatuh ke tangan yang salah dan disalahgunakan (Weber, 2010). Misalnya, data yang dikumpulkan oleh perangkat IoT di rumah, seperti penggunaan energi atau pola tidur, bisa memberikan gambaran detail tentang kebiasaan dan gaya hidup pengguna.

Penyalahgunaan data ini bisa berupa pemasaran yang tidak diinginkan, penipuan, atau bahkan pemantauan dan pengintaian yang tidak sah. Selain itu, jika perangkat IoT tidak aman, data yang dikumpulkan bisa diretas dan

digunakan untuk tujuan jahat. Misalnya, perangkat IoT yang digunakan dalam sistem kesehatan bisa mengandung informasi sensitif tentang kondisi kesehatan pengguna, yang jika disalahgunakan, bisa memiliki konsekuensi serius.

Upaya untuk melindungi privasi pengguna dan mencegah penyalahgunaan data melibatkan implementasi mekanisme keamanan yang kuat, termasuk enkripsi data, kontrol akses yang ketat, dan transparansi dalam pengumpulan dan penggunaan data (Sicari *et al.*, 2015). Selain itu, perlu ada regulasi dan kebijakan yang jelas untuk melindungi data pengguna. Meskipun ada tantangan yang signifikan, melindungi privasi pengguna dalam IoT adalah prioritas utama dalam era transformasi digital ini.

2. Pemantauan yang tidak sah

Salah satu bentuk penyalahgunaan data dalam Internet of Things (IoT) yang sangat meresahkan adalah pemantauan tidak sah atau ilegal. Kebutuhan akan data untuk memberikan layanan yang lebih baik dan efisien seringkali berujung pada pengumpulan dan analisis data secara besar-besaran, yang membuka peluang untuk pemantauan tidak sah (Miorandi *et al.*, 2012). Hal ini diperparah dengan fakta bahwa banyak perangkat IoT, seperti kamera keamanan atau perangkat pelacak, secara langsung dapat digunakan untuk pemantauan. Jika perangkat-perangkat ini dikendalikan oleh pihak yang tidak berwenang, maka privasi pengguna bisa sangat terancam.

Pemantauan tidak sah tidak hanya terbatas pada tindakan oleh penjahat cyber, tetapi juga bisa dilakukan oleh perusahaan atau pemerintah (Atzori, Iera and Morabito, 2010). Misalnya, perusahaan bisa memantau perilaku konsumen mereka untuk tujuan pemasaran, atau pemerintah bisa melakukan pemantauan untuk tujuan keamanan nasional. Meski ada situasi di mana pemantauan

ini mungkin diperlukan, tanpa kontrol yang ketat dan transparansi, pemantauan bisa menjadi alat yang melanggar privasi.

Untuk mengatasi masalah ini, penting untuk mendefinisikan batas-batas etika dan hukum terkait pemantauan dalam konteks IoT. Selain itu, perangkat IoT harus dilengkapi dengan fitur keamanan yang mampu melindungi pengguna dari pemantauan ilegal. Pengguna juga harus diberi kontrol lebih atas data mereka, termasuk siapa yang bisa mengakses data dan untuk tujuan apa. Menghadapi tantangan ini adalah bagian penting dalam mewujudkan potensi penuh dari IoT, tanpa mengorbankan hak privasi pengguna.

8.2.3 Kasus Nyata: Ancaman dan Implikasi dalam Dunia Nyata

Salah satu kasus yang menjadi sorotan adalah serangan DDoS (*Distributed Denial of Service*) yang ditujukan kepada Dyn, sebuah perusahaan DNS, pada Oktober 2016. Serangan ini mengeksploitasi kerentanan keamanan pada berbagai perangkat IoT, seperti kamera CCTV dan DVR, untuk melumpuhkan sejumlah situs web besar seperti Twitter, Netflix, dan Reddit. Implikasi dari serangan ini sangat signifikan, menciptakan gangguan layanan internet pada skala yang belum pernah terjadi sebelumnya, dan membuka mata dunia terhadap potensi risiko serangan cyber melalui perangkat IoT (Kolias *et al.*, 2017).

Selain itu, ada juga kasus perangkat medis yang disasar oleh peretas. Pada tahun 2017, perangkat pacemaker buatan St. Jude Medical terbukti memiliki kerentanan yang memungkinkan peretas mengendalikan perangkat tersebut. Meski tidak ada laporan korban jiwa akibat serangan ini, implikasinya sangat mengejutkan dan meresahkan. Pasien yang menggunakan perangkat ini berisiko menjadi korban serangan jantung buatan jika perangkat mereka diretas (Kruse *et al.*, 2017).

Ancaman privasi juga menjadi masalah serius dalam IoT. Salah satunya adalah kasus Amazon Echo, sebuah perangkat yang dilengkapi dengan asisten virtual Alexa, yang terlibat dalam penyelidikan kasus pembunuhan pada tahun 2015. Polisi meminta akses ke rekaman Alexa, berargumen bahwa data tersebut mungkin berisi bukti penting. Kasus ini memunculkan pertanyaan serius tentang sejauh mana perangkat IoT dapat mengumpulkan dan menyimpan informasi pribadi penggunanya, dan siapa yang seharusnya memiliki hak akses ke data tersebut (Wang, 2016).

Kasus-kasus ini menggambarkan beberapa ancaman nyata yang dihadapi oleh pengguna perangkat IoT, dan bagaimana ancaman tersebut bisa memiliki implikasi signifikan dalam kehidupan nyata. Mereka menunjukkan bahwa upaya untuk mengamankan IoT adalah tantangan yang kompleks, yang memerlukan solusi holistik yang melibatkan peningkatan keamanan perangkat, edukasi pengguna, dan regulasi yang lebih kuat.

8.3 Prinsip-prinsip Keamanan dan Privasi dalam IoT

Prinsip-prinsip keamanan dan privasi menjadi pondasi penting dalam penerapan dan pengembangan Internet of Things (IoT). Mengingat IoT menyangkut koneksi antar perangkat dalam skala yang luas, potensi ancaman dan kerentanan yang ada menjadi sangat tinggi. Selain itu, volume data yang dihasilkan dan diproses oleh perangkat IoT sering kali mengandung informasi pribadi dan sensitif pengguna, sehingga perlindungan privasi menjadi pertimbangan utama. Pada bagian ini, kita akan membahas prinsip-prinsip dasar keamanan dan privasi dalam IoT, yang mencakup rancangan keamanan, prinsip minimalisasi data, dan prinsip transparansi.

8.3.1 Rancangan Keamanan (Security by Design)

Rancangan Keamanan atau *Security by Design* adalah konsep penting dalam dunia *Internet of Things* (IoT) yang menekankan pentingnya peran keamanan sejak dini dalam proses perancangan sistem. Pendekatan ini memungkinkan identifikasi dan mitigasi potensi ancaman sebelum sistem benar-benar beroperasi (Jordan, 2019). Prinsip ini mendorong pengembang untuk mempertimbangkan aspek keamanan sebagai bagian integral dari proses desain, bukan sebagai tambahan atau modifikasi di belakang.

Penerapan *Security by Design* mengurangi risiko kerentanan sistem yang mungkin bisa disalahgunakan oleh peretas. Sebuah penelitian mencatat bahwa serangan cyber pada perangkat IoT seringkali disebabkan oleh kerentanan yang dapat dicegah jika pertimbangan keamanan telah diterapkan sejak awal (Alrawais *et al.*, 2017). Dengan demikian, pentingnya prinsip ini dalam memastikan keamanan sistem IoT tidak dapat diremehkan.

Security by Design merupakan pendekatan yang menekankan pada perlunya integrasi elemen-elemen keamanan sejak awal pembuatan sistem. Bukan sebagai tambahan atau patch yang ditambahkan setelah sistem dikembangkan atau saat terjadi masalah. Konsep ini mencakup sejumlah aspek penting dalam desain dan pengembangan sistem, termasuk perangkat keras, perangkat lunak, dan protokol jaringan.

Pertama, dalam aspek perangkat keras, *Security by Design* berarti bahwa setiap komponen perangkat keras yang digunakan dalam sistem harus dianggap sebagai potensi titik masuk untuk serangan. Oleh karena itu, setiap komponen tersebut harus dirancang dengan pertimbangan keamanan, dan diberikan perlindungan yang sesuai.

Kedua, dalam aspek perangkat lunak, *Security by Design* menuntut bahwa setiap bagian kode yang ditulis harus aman dari segi keamanan. Ini melibatkan penerapan prinsip-prinsip seperti penggunaan teknik pemrograman yang aman, melakukan review

kode secara berkala untuk menemukan dan memperbaiki potensi kerentanan, dan penerapan kontrol akses yang tepat.

Ketiga, dalam aspek jaringan, *Security by Design* berarti bahwa protokol komunikasi yang digunakan harus dirancang sedemikian rupa untuk mencegah serangan seperti pemalsuan identitas, penyadapan, dan gangguan pada integritas data.

Selain itu, *Security by Design* juga melibatkan penerapan prinsip keamanan lainnya seperti Prinsip Hak Akses Terkecil, dimana akses ke sumber daya sistem diberikan sesuai dengan apa yang diperlukan oleh pengguna atau proses, dan tidak lebih.

Selanjutnya, konsep ini juga menuntut pengujian keamanan yang berkelanjutan dan pembaruan reguler terhadap sistem untuk memastikan bahwa sistem tetap aman seiring dengan berkembangnya teknologi dan taktik serangan. Dengan demikian, *Security by Design* menawarkan pendekatan holistik terhadap keamanan sistem, dan membantu memastikan bahwa keamanan adalah bagian yang melekat dan integral dari sistem tersebut, bukan hanya sebagai tambahan.

8.3.2 Prinsip Minimalisasi Data (Data Minimization)

Prinsip Minimalisasi Data atau *Data Minimization* adalah suatu prinsip yang mendorong untuk membatasi pengumpulan data menjadi sesedikit mungkin dan hanya sebanyak yang diperlukan. Prinsip ini bertujuan untuk mengurangi resiko terkait privasi dan keamanan yang mungkin timbul dari penanganan dan penyimpanan data. Dalam konteks *Internet of Things* (IoT), prinsip ini menjadi sangat relevan mengingat IoT kerap melibatkan pengumpulan dan pengolahan data dalam skala besar.

Pada dasarnya, *Data Minimization* berfokus pada konsep bahwa semakin sedikit data yang dikumpulkan dan disimpan, semakin sedikit pula peluang terjadinya penyalahgunaan data atau kebocoran data. Dengan mengurangi jumlah data yang disimpan, perusahaan dapat mengurangi resiko dan tanggung jawab terkait penanganan data tersebut. Prinsip ini berlaku baik untuk data

pelanggan, data perusahaan, maupun data sistem (European Data Protection Board, 2019).

Prinsip Minimalisasi Data, atau Data Minimization, merujuk pada batasan dalam pengumpulan data hanya pada tingkat yang absolut diperlukan. Untuk memahami penerapan prinsip ini, mari kita ambil contoh perangkat IoT seperti smart speaker. Perangkat ini secara konstan menerima dan memproses data suara, namun dalam prakteknya tidak semua data tersebut perlu disimpan. Oleh karena itu, produsen perangkat seharusnya merancang sistem yang secara otomatis menghapus data suara yang tidak diperlukan setelah memprosesnya. Hal ini berarti hanya data yang benar-benar esensial untuk fungsi perangkat yang disimpan.

Implementasi prinsip ini juga harus diterapkan dalam perancangan sistem dan produk. Misalnya, saat merancang formulir online, perusahaan harus hanya meminta informasi yang benar-benar diperlukan untuk proses tersebut. Data seperti tanggal lahir atau alamat rumah mungkin tidak perlu dikumpulkan jika itu tidak relevan untuk layanan atau produk yang ditawarkan.

Selain itu, prinsip ini juga berarti bahwa data harus dihapus secara rutin setelah tidak lagi diperlukan. Jika suatu perusahaan mengumpulkan data pelanggan untuk tujuan tertentu dan tujuan tersebut telah tercapai, maka data tersebut harus dihapus dari sistem mereka. Ini akan membantu mencegah penyalahgunaan data dan melindungi privasi pelanggan (European Data Protection Board, 2019).

Namun, penerapan prinsip ini tidak serta merta meniadakan kebutuhan untuk keamanan data. Sebaliknya, perusahaan perlu menerapkan langkah-langkah keamanan yang tepat untuk melindungi data yang mereka miliki, termasuk enkripsi data, kontrol akses yang ketat, dan pemantauan aktivitas yang mencurigakan. Data Minimization bukan berarti mengabaikan pentingnya keamanan data, melainkan menjadi salah satu langkah dalam strategi keamanan data yang lebih komprehensif.

Terakhir, prinsip ini juga memandu organisasi dalam menyeimbangkan antara kebutuhan untuk mengumpulkan dan menggunakan data dengan tanggung jawab mereka dalam melindungi privasi individu. Dalam konteks ini, organisasi perlu memastikan bahwa mereka tidak hanya mematuhi hukum dan regulasi terkait perlindungan data, tetapi juga memperhatikan etika dan kepatutan dalam pengumpulan dan penggunaan data.

8.3.3 Prinsip Transparansi (Transparency)

Prinsip Transparansi atau *Transparency* dalam konteks *Internet of Things* (IoT) merujuk pada kewajiban perusahaan dan organisasi untuk jujur dan terbuka tentang bagaimana mereka mengumpulkan, menggunakan, dan membagikan data. Transparansi tidak hanya penting untuk membangun kepercayaan pengguna, tapi juga menjadi bagian penting dari regulasi privasi data seperti *General Data Protection Regulation* (GDPR) di Uni Eropa.

Dalam praktiknya, transparansi dapat diimplementasikan melalui berbagai cara. Salah satu cara yang paling umum adalah dengan menyediakan kebijakan privasi yang mudah dipahami. Kebijakan ini harus menjelaskan dengan jelas jenis data apa yang dikumpulkan, bagaimana data tersebut digunakan, dan siapa yang mungkin dapat mengakses data tersebut. Selain itu, perusahaan harus transparan tentang bagaimana pengguna dapat mengontrol dan mengelola data mereka.

Dalam penerapannya, prinsip transparansi dalam IoT dapat diterapkan dalam beberapa cara. Pertama, melalui penyediaan Kebijakan Privasi yang jelas dan mudah dipahami. Dokumen ini harus menjelaskan secara terperinci tentang jenis data yang dikumpulkan, tujuan pengumpulan, cara pengolahan data, siapa saja yang dapat mengakses data tersebut, dan bagaimana pengguna dapat mengontrol dan mengelola data mereka sendiri.

Kedua, melalui komunikasi proaktif. Jika ada perubahan dalam cara pengumpulan atau penggunaan data, pengguna harus

segera diberi tahu. Selain itu, jika terjadi pelanggaran data, perusahaan harus segera memberi tahu pengguna, mencakup detail tentang apa yang terjadi, data apa yang terpengaruh, dan apa langkah-langkah yang dapat diambil oleh pengguna.

Ketiga, melalui pendekatan inovatif dalam menyampaikan transparansi, seperti melalui aplikasi seluler atau situs web. Perangkat IoT seringkali memiliki antarmuka pengguna yang minimalis dan terbatas, sehingga penyampaian informasi transparansi harus kreatif dan efektif.

Tujuan akhir dari prinsip transparansi bukan hanya keterbukaan informasi, tetapi juga pemberdayaan pengguna dalam mengontrol dan melindungi data mereka sendiri. Dengan transparansi, pengguna dapat membuat keputusan yang lebih baik dan informasi tentang bagaimana mereka berinteraksi dengan teknologi, termasuk IoT.

8.4 Strategi dan Teknologi untuk Mengamankan IoT

8.4.1 Proteksi Jaringan dan Sistem

Proteksi jaringan dan sistem merupakan komponen penting dalam strategi keamanan IoT. Salah satu metode yang banyak digunakan adalah segmentasi jaringan, yang berfungsi untuk memisahkan perangkat IoT dari jaringan utama perusahaan atau rumah. Hal ini dapat membantu mencegah penyebaran ancaman jika satu perangkat dikompromikan. Segmentasi juga memfasilitasi pemantauan yang lebih efektif terhadap aktivitas yang mencurigakan dalam jaringan (Shieh, 2014).

Pada tingkat sistem, manajemen patch dan pembaruan perangkat keras dan lunak juga sangat penting. Perangkat IoT harus selalu diperbarui dengan versi perangkat keras dan perangkat lunak terbaru untuk menangkal ancaman baru yang terus berkembang. Proses ini seringkali menjadi tantangan karena

volume perangkat dalam jaringan IoT bisa sangat besar, sehingga otomatisasi dapat menjadi solusi efektif (Kolias *et al.*, 2017).

Selain itu, penggunaan teknologi keamanan yang lebih lanjut seperti *Intrusion Detection System* (IDS) dan *Intrusion Prevention System* (IPS) juga dapat meningkatkan proteksi sistem dan jaringan. IDS dan IPS bekerja dengan memantau lalu lintas jaringan dan mengidentifikasi pola yang mencurigakan atau aktivitas yang melanggar kebijakan keamanan (Zarpelão *et al.*, 2017).

Akhirnya, prinsip '*Security by Design*' harus diterapkan dalam pengembangan dan penyebaran perangkat IoT. Ini berarti bahwa keamanan harus menjadi bagian integral dari desain produk dan bukan hanya sebagai tambahan setelah produk dikembangkan. Hal ini memastikan bahwa keamanan terintegrasi di semua tingkatan sistem dan jaringan.

8.4.2 Manajemen Identitas dan Akses

Manajemen Identitas dan Akses (*Identity and Access Management/IAM*) adalah elemen kunci dalam strategi keamanan IoT. Dalam konteks IoT, IAM melibatkan pengaturan dan pengelolaan identitas digital yang unik untuk setiap perangkat yang terhubung ke jaringan. Selain itu, proses ini juga mencakup pengendalian akses ke jaringan dan data yang diproses oleh perangkat-perangkat ini. Dengan demikian, hanya perangkat dan pengguna yang berwenang yang dapat mengakses dan berinteraksi dengan sistem (Roman, Najera and Lopez, 2011).

Fungsi utama IAM adalah untuk mencegah akses yang tidak sah ke sistem. Untuk mencapai hal ini, metode autentikasi kuat seperti otentikasi dua faktor (2FA) dan multi-faktor (MFA) sering digunakan. Otentikasi ini melibatkan penggunaan lebih dari satu metode verifikasi untuk memastikan identitas pengguna atau perangkat sebelum memberikan akses.

Di samping itu, kebijakan akses juga perlu dikelola dengan hati-hati. Kebijakan ini menentukan siapa yang dapat mengakses

apa dan kapan mereka dapat melakukannya. Selain itu, kebijakan ini juga perlu diperbarui secara berkala untuk mencerminkan perubahan dalam lingkungan dan ancaman keamanan. Misalnya, jika perangkat atau pengguna dikompromikan, kebijakan tersebut perlu diperbarui untuk mencegah akses lebih lanjut oleh pihak yang tidak berwenang.

Dalam konteks *Internet of Things* (IoT), prinsip Manajemen Identitas dan Akses (IAM) memiliki tingkat kompleksitas yang lebih tinggi dibandingkan dengan aplikasinya dalam sistem komputasi tradisional. Hal ini disebabkan oleh beberapa karakteristik unik IoT, seperti heterogenitas perangkat, skalabilitas yang besar, dan komunikasi mesin-ke-mesin yang berkelanjutan (Xiao *et al.*, 2018).

Jaringan IoT, yang mencakup berbagai perangkat dari berbagai vendor dan model, sering kali memiliki standar dan protokol keamanan yang berbeda-beda. Oleh karena itu, solusi IAM untuk IoT harus mampu mendukung berbagai protokol autentikasi dan otorisasi. Selain itu, karena IoT melibatkan komunikasi antar perangkat tanpa intervensi manusia, metode autentikasi harus efisien dan aman dari ancaman seperti pemalsuan identitas dan serangan replay.

Skalabilitas adalah tantangan lain dalam menerapkan IAM pada IoT. Dengan jutaan perangkat IoT yang saling berkomunikasi, solusi IAM harus mampu mengelola volume permintaan autentikasi dan otorisasi yang besar dalam waktu nyata. Selain itu, solusi IAM harus mampu melakukan pembaruan dan perubahan kebijakan keamanan dengan cepat dan efisien.

Untuk mengatasi tantangan ini, banyak solusi IAM IoT saat ini mengandalkan teknologi seperti Blockchain dan Machine Learning. Blockchain dapat digunakan untuk menciptakan sistem autentikasi terdistribusi dan transparan, di mana setiap perangkat memiliki identitas digital yang unik dan tak bisa dipalsukan. Sementara itu, Machine Learning dapat digunakan untuk

mendeteksi aktivitas mencurigakan dan melakukan penyesuaian kebijakan keamanan secara otomatis (Makhdoom *et al.*, 2019).

8.4.3 Teknologi Kriptografi

Teknologi kriptografi adalah salah satu metode utama untuk memastikan keamanan dan privasi dalam *Internet of Things* (IoT). Kriptografi memberikan lapisan perlindungan data penting, baik dalam transmisi maupun penyimpanan, sehingga dapat mencegah akses oleh pihak-pihak yang tidak berhak (SathishKumar and R. Patel, 2014). Dalam IoT, teknologi ini digunakan dalam berbagai cara, seperti untuk autentikasi perangkat, integritas data, dan privasi komunikasi.

Metode kriptografi yang umum digunakan dalam IoT adalah enkripsi simetris dan asimetris. Enkripsi simetris, seperti AES, digunakan untuk melindungi data dalam transmisi antar perangkat IoT. Sementara itu, enkripsi asimetris, seperti RSA, digunakan untuk autentikasi perangkat dan penandatanganan digital. Meski begitu, kedua jenis enkripsi ini memiliki tantangan tersendiri, seperti isu-isu terkait efisiensi komputasi dan pengelolaan kunci.

Untuk menjawab tantangan ini, solusi kriptografi ringan seringkali menjadi pilihan utama. Kriptografi ringan dirancang untuk bekerja efisien pada perangkat IoT yang memiliki keterbatasan dalam hal daya komputasi, memori, dan daya baterai. Beberapa algoritma kriptografi ringan yang umum digunakan adalah PRESENT dan SPECK.

Meski begitu, teknologi kriptografi dalam IoT masih memiliki tantangan-tantangan lain yang perlu ditangani. Contohnya, proses pengelolaan kunci yang efisien dan aman, serta penyesuaian dengan perubahan kebijakan keamanan dan standar. Oleh karena itu, penelitian dan pengembangan lebih lanjut di bidang ini masih sangat dibutuhkan.

Salah satu contoh tantangan lainnya dalam penerapan kriptografi pada IoT adalah keterbatasan sumber daya perangkat.

Banyak perangkat IoT memiliki kapabilitas pemrosesan dan memori yang terbatas, sehingga tidak mampu menjalankan algoritma kriptografi yang kompleks dan berat. Oleh karena itu, para peneliti terus mencari dan mengembangkan algoritma kriptografi yang lebih ringan dan efisien, namun tetap aman.

Selain itu, manajemen kunci kriptografi juga menjadi tantangan besar dalam IoT. Mengingat jumlah perangkat IoT yang sangat banyak dan dapat berubah-ubah, pengelolaan kunci kriptografi dapat menjadi sangat rumit. Skema manajemen kunci yang efisien dan scalable sangat dibutuhkan dalam konteks IoT.

Meski ada tantangan, teknologi kriptografi tetap menjadi bagian penting dalam menjaga keamanan dan privasi IoT. Dalam banyak kasus, kriptografi bukan hanya digunakan untuk melindungi data, tetapi juga untuk melakukan autentikasi perangkat dan pengguna, serta untuk memastikan integritas data dan non-repudiasi transaksi.

Sebagai bagian dari strategi dan teknologi untuk mengamankan IoT, penelitian dan pengembangan kriptografi harus dilakukan secara berkelanjutan. Termasuk di dalamnya adalah pengembangan standar dan protokol keamanan yang berbasis kriptografi, yang dapat digunakan untuk membangun dan mengoperasikan jaringan IoT yang aman dan dapat dipercaya.

8.5 Regulasi dan Standar Keamanan dan Privasi IoT

8.5.1 Overview Regulasi Yang Ada

Regulasi dan standar terkait keamanan dan privasi dalam *Internet of Things* (IoT) berperan penting dalam menjaga keamanan dan privasi pengguna. Regulasi merupakan aturan hukum yang dibuat oleh otoritas pemerintah untuk menjaga keamanan dan privasi data pengguna, sedangkan standar adalah aturan teknis yang dirancang untuk memastikan interoperabilitas dan keamanan sistem. Untuk mengatur dan menjaga ekosistem

IoT, berbagai negara telah mengembangkan regulasi dan standar mereka sendiri.

Di Amerika Serikat, *Federal Trade Commission* (FTC) secara aktif mencoba untuk menjaga langkah dengan perubahan teknologi. Mereka telah mengeluarkan panduan keamanan yang mendalam untuk produsen perangkat IoT, mencakup berbagai aspek seperti desain perangkat, penggunaan enkripsi, pembaruan perangkat lunak yang aman, dan penggunaan autentikasi yang kuat. Ini menunjukkan bahwa regulasi yang ada harus tetap fleksibel dan adaptif terhadap perkembangan teknologi.

Di Uni Eropa, *General Data Protection Regulation* (GDPR) adalah salah satu regulasi yang sangat penting. GDPR mencakup sejumlah besar aspek keamanan dan privasi termasuk IoT. Ini menetapkan aturan yang ketat tentang bagaimana data pribadi dapat dikumpulkan, disimpan, diproses, dan dibagikan. Peraturan ini memiliki implikasi yang jauh mencapai bagi perusahaan di seluruh dunia yang menangani data warga Uni Eropa. Meski demikian, implementasi GDPR dalam konteks IoT juga memiliki tantangan tersendiri, terutama terkait dengan prinsip minimalisasi data dan konsen yang tepat dalam pengumpulan data.

Standar keamanan dan privasi juga sangat penting dalam IoT. Organisasi seperti *International Organization for Standardization* (ISO) dan *Internet Engineering Task Force* (IETF) telah bekerja untuk mengembangkan standar keamanan dan privasi IoT. Standar ini dirancang untuk memastikan interoperabilitas dan keamanan sistem, serta untuk memandu produsen dalam mendesain dan membangun perangkat yang aman dan dapat dipercaya.

8.5.2 Standar Keamanan IoT

Berbicara tentang standar keamanan IoT, sejumlah organisasi internasional memiliki peran penting dalam pembentukan standar tersebut. Misalnya, *International Organization for Standardization* (ISO) dan *Internet Engineering*

Task Force (IETF) telah bekerja untuk membangun standar keamanan IoT. Kedua organisasi ini telah merancang serangkaian standar yang bertujuan untuk memastikan keamanan dan privasi dalam ekosistem IoT. Ini mencakup standar untuk desain perangkat, jaringan, dan aplikasi, serta standar untuk pengelolaan data dan privasi.

Organisasi standar lainnya seperti *Institute of Electrical and Electronics Engineers* (IEEE) juga telah aktif dalam membangun standar keamanan IoT. Sebagai contoh, IEEE telah merilis IEEE 2413, standar arsitektur untuk *Internet of Things* (IoT) yang menyediakan kerangka untuk keamanan, privasi, dan interoperabilitas perangkat IoT. Standar ini mencakup berbagai aspek termasuk autentikasi, kontrol akses, integritas data, dan privasi data.

Selain itu, *National Institute of Standards and Technology* (NIST) juga memainkan peran penting dalam pembentukan standar keamanan IoT. NIST telah merilis draft panduan keamanan IoT, NISTIR 8259, yang memberikan rekomendasi keamanan khusus untuk produsen perangkat IoT. Panduan ini mencakup sejumlah rekomendasi untuk pemantauan keamanan, pembaruan perangkat lunak, dan penanganan data yang aman.

Meski demikian, penerapan standar ini tidak tanpa tantangan. Salah satu tantangan utama adalah keanekaragaman perangkat IoT dan penggunaannya, yang membuat sulit untuk menerapkan satu set standar yang sama untuk semua kasus. Selain itu, banyak produsen perangkat IoT tidak memiliki pengetahuan atau sumber daya untuk menerapkan standar keamanan ini, dan beberapa mungkin memilih untuk mengabaikannya demi kecepatan masuk pasar dan biaya yang lebih rendah. Oleh karena itu, upaya tambahan diperlukan untuk mendidik produsen tentang pentingnya keamanan IoT dan untuk mengembangkan cara-cara efektif untuk menerapkan dan mematuhi standar ini.

Standar keamanan IoT ideal harus mencakup berbagai aspek, dari desain dan produksi hingga pemantauan dan

pemeliharaan perangkat. Berikut adalah beberapa hal yang harus menjadi bagian dari standar keamanan IoT:

1. Rancangan Keamanan: Keamanan harus menjadi bagian integral dari proses desain perangkat IoT, bukan hanya tambahan belakangan. Ini termasuk pendekatan '*security by design*' dan '*privacy by design*', di mana aspek keamanan dan privasi dipertimbangkan dan diimplementasikan selama fase desain produk.
2. Enkripsi dan Otentikasi: Data yang dihasilkan oleh perangkat IoT harus dienkripsi, dan mekanisme otentikasi yang kuat harus digunakan untuk memastikan bahwa hanya perangkat dan pengguna yang sah yang dapat mengakses data.
3. Manajemen Identitas dan Akses: Standar harus mencakup pengaturan untuk kontrol akses yang efektif, yang memungkinkan pengguna dan perangkat untuk mengakses data dan fungsi hanya sejauh yang mereka butuhkan.
4. Pembaruan dan Patching: Perangkat IoT harus memiliki mekanisme untuk pembaruan dan patching perangkat lunak, yang memungkinkan produsen untuk memperbaiki celah keamanan dan bug segera setelah mereka ditemukan.
5. Ketahanan terhadap Serangan: Perangkat IoT harus dirancang untuk bertahan terhadap berbagai jenis serangan, termasuk DDoS, *man-in-the-middle*, dan serangan fisik.
6. Proteksi Data dan Privasi: Standar harus memastikan bahwa data pengguna dilindungi dan bahwa privasi pengguna dihormati, termasuk membatasi pengumpulan dan penggunaan data, dan memastikan transparansi dalam bagaimana data digunakan.
7. Audit dan Pemantauan: Perangkat IoT harus memiliki kapabilitas untuk logging dan pemantauan, yang memungkinkan deteksi dan respon terhadap insiden keamanan.

8. Kompatibilitas dan Interoperabilitas: Standar keamanan IoT harus kompatibel dengan standar keamanan yang ada dan memungkinkan interoperabilitas antara perangkat dan sistem yang berbeda.
9. Kesadaran Pengguna: Standar juga harus mempromosikan kesadaran keamanan di antara pengguna perangkat IoT, termasuk pendidikan tentang risiko keamanan dan cara mengelolanya.

Standar ini, jika diimplementasikan dengan baik, dapat membantu melindungi perangkat IoT dari berbagai ancaman dan memastikan bahwa mereka dapat digunakan dengan aman dan efektif.

8.5.3 Dampak dan Tantangan Implementasi Regulasi Dan Standar

Implementasi regulasi dan standar dalam *Internet of Things* (IoT) memiliki dampak dan tantangan tersendiri. Pada satu sisi, penerapan regulasi dan standar dapat menjamin tingkat minimum keamanan dan privasi dalam sistem IoT. Sebagai contoh, regulasi seperti *General Data Protection Regulation* (GDPR) di Uni Eropa memaksa perusahaan untuk menangani data pengguna dengan lebih baik dan bertanggung jawab, sementara standar seperti yang dikeluarkan oleh *Institute of Electrical and Electronics Engineers* (IEEE) atau *International Organization for Standardization* (ISO) menyediakan kerangka kerja untuk merancang dan mengimplementasikan sistem IoT yang aman.

Di sisi lain, implementasi regulasi dan standar dapat menjadi tantangan yang signifikan, terutama bagi perusahaan kecil dan startup yang mungkin tidak memiliki sumber daya yang diperlukan untuk mematuhi regulasi dan standar yang kompleks dan beragam ini. Beban kepatuhan ini dapat membatasi inovasi dan memperlambat adopsi IoT, terutama di sektor-sektor yang belum sepenuhnya memahami manfaat teknologi ini.

Selain itu, meskipun regulasi dan standar dapat membantu memitigasi sejumlah risiko keamanan dan privasi, mereka tidak bisa menjamin keamanan dan privasi secara absolut. Hal ini terutama berlaku dalam konteks IoT, di mana ancaman terus berkembang dan perangkat sering kali memiliki umur panjang yang berarti mereka mungkin harus berurusan dengan ancaman yang tidak ada pada saat mereka dirancang dan diproduksi. Dengan demikian, penting untuk melihat regulasi dan standar sebagai bagian dari solusi keamanan dan privasi IoT yang lebih besar, dan bukan sebagai solusi yang sempurna.

Terakhir, ada tantangan dalam memastikan bahwa regulasi dan standar diterapkan secara konsisten di seluruh dunia. Dengan adanya banyak negara dan wilayah yang menerapkan regulasi dan standar mereka sendiri, ada risiko fragmentasi yang dapat menghambat interoperabilitas dan mempersulit perusahaan yang beroperasi di berbagai pasar untuk mematuhi semua regulasi dan standar yang berbeda ini.

8.6 Tantangan dan Solusi Masa Depan untuk Keamanan dan Privasi IoT

8.6.1 Tantangan Dalam Implementasi Keamanan Dan Privasi IoT

Implementasi keamanan dan privasi dalam *Internet of Things* (IoT) tentu menimbulkan tantangan tersendiri. Tantangan pertama adalah heterogenitas dan kompleksitas sistem IoT. IoT terdiri dari berbagai perangkat dan aplikasi dari berbagai produsen dengan standar dan protokol yang berbeda-beda. Menyelaraskan semua komponen ini menjadi satu sistem yang aman adalah tugas yang sangat kompleks. Selain itu, kerentanan yang ada dalam satu perangkat atau aplikasi dapat menjadi pintu masuk bagi penyerang untuk merusak seluruh sistem.

Tantangan kedua adalah kurangnya kesadaran pengguna terhadap keamanan dan privasi dalam IoT. Banyak pengguna yang

belum sepenuhnya memahami risiko dan ancaman yang ada, sehingga mereka mungkin tidak mengambil langkah-langkah pencegahan yang diperlukan. Misalnya, pengguna mungkin menggunakan password yang lemah atau bahkan tidak mengubah password default pada perangkat IoT mereka. Situasi ini dapat memudahkan penyerang untuk mendapatkan akses ke perangkat dan data pengguna.

Ketiga, karena sifat IoT yang menghubungkan berbagai perangkat dan sistem dalam jaringan, ancaman keamanan pada satu titik dapat berdampak pada keseluruhan sistem. Dengan kata lain, IoT menciptakan efek domino dalam hal keamanan, di mana satu titik kerentanan dapat digunakan untuk menyerang dan mengkompromikan bagian lain dari sistem. Ini berarti bahwa strategi keamanan harus melibatkan perlindungan komprehensif di seluruh jaringan, bukan hanya pada titik-titik tertentu.

Keempat, ada tantangan dalam menyeimbangkan antara kebutuhan akan keamanan dan privasi dengan kebutuhan akan fungsi dan kinerja. Mengimplementasikan fitur keamanan yang kuat dapat memengaruhi kinerja perangkat IoT dan mempersulit penggunaan. Misalnya, penggunaan teknologi enkripsi yang kuat dapat memperlambat transfer data dan mengurangi daya tahan baterai pada perangkat IoT.

8.6.2 Solusi Yang Dikembangkan Untuk Keamanan Dan Privasi IoT

Untuk mengatasi tantangan dalam keamanan dan privasi IoT, berbagai solusi telah dikembangkan. Pertama, peningkatan standarisasi dalam IoT dapat membantu menangani isu heterogenitas dan kompleksitas. Standar yang diterapkan secara luas dapat memastikan kompatibilitas dan interoperabilitas antara berbagai perangkat dan aplikasi, memudahkan implementasi keamanan yang konsisten di seluruh sistem. Standar juga dapat memberikan pedoman bagi produsen tentang fitur keamanan minimal yang harus ada dalam setiap perangkat IoT.

Kedua, pendidikan dan penyadaran pengguna sangat penting. Pengguna harus diajarkan tentang risiko dan ancaman keamanan dalam IoT dan bagaimana mereka dapat melindungi diri mereka sendiri. Ini bisa mencakup pengetahuan tentang pentingnya menggunakan password yang kuat dan mengubah password default, serta pemahaman tentang privasi dan pengaturan keamanan pada perangkat IoT mereka. Selain itu, produsen perangkat juga harus memastikan bahwa mereka memberikan informasi yang jelas dan mudah dipahami tentang fitur keamanan dan privasi perangkat mereka.

Ketiga, peningkatan teknologi keamanan dan metode deteksi ancaman juga dapat membantu melindungi IoT dari ancaman. Teknologi seperti enkripsi, otentikasi, dan teknologi Blockchain, dapat digunakan untuk melindungi data dan menjaga integritas dan kerahasiaannya. Selain itu, penggunaan teknologi deteksi ancaman dan respons terhadap insiden dapat membantu mendeteksi dan merespons secara cepat terhadap ancaman yang ada.

Keempat, pembuatan dan penegakan regulasi dan standar keamanan IoT yang kuat oleh pemerintah dan organisasi internasional dapat membantu memastikan bahwa produsen perangkat IoT memenuhi standar keamanan minimal. Regulasi juga dapat mendorong transparansi dan akuntabilitas dari produsen perangkat IoT, memastikan bahwa mereka bertanggung jawab untuk menjaga keamanan dan privasi pengguna.0020

8.6.3 Prediksi Tren Masa Depan Untuk Keamanan Dan Privasi IoT

Menatap masa depan, ada beberapa tren yang dapat kita prediksi dalam ranah keamanan dan privasi Internet of Things (IoT). Pertama, kita dapat melihat peningkatan fokus pada solusi keamanan yang lebih kuat untuk IoT. Dengan pertumbuhan eksponensial dalam jumlah perangkat IoT, permintaan untuk teknologi keamanan yang lebih baik dan lebih canggih akan

meningkat. Setiap perangkat yang terhubung merupakan potensi titik masuk untuk perangkat jahat; oleh karena itu, tuntutan akan ada pada pengembangan alat dan teknologi yang dapat secara efektif mencegah serangan, mendeteksi mereka secepat mungkin jika mereka terjadi, dan merespon mereka dengan cara yang mengurangi dampak buruknya. Peningkatan ini dapat mencakup penelitian dan pengembangan lebih lanjut tentang metode enkripsi, otentikasi, dan deteksi intrusi.

Kedua, AI dan machine learning akan memainkan peran yang semakin besar dalam keamanan IoT. Melalui penggunaan algoritma yang mampu belajar dari data dan memprediksi perilaku berdasarkan pola yang ditemukan, AI dapat memungkinkan deteksi ancaman yang lebih cepat dan lebih tepat. Selain itu, AI juga bisa digunakan untuk memprediksi ancaman dan serangan masa depan, memberikan lapisan keamanan proaktif yang sangat dibutuhkan dalam IoT.

Ketiga, teknologi seperti blockchain akan semakin penting dalam konteks IoT. Blockchain, dengan karakteristik desentralisasi dan transparansi, memberikan solusi yang menjanjikan untuk tantangan yang dihadapi dalam aspek keamanan dan privasi IoT. Teknologi ini bisa digunakan untuk melacak dan mengaudit transaksi antara perangkat IoT, membuat jaringan menjadi lebih aman dan sulit untuk diserang atau dimanipulasi.

Keempat, kita dapat mengantisipasi peningkatan regulasi dan standar keamanan untuk perangkat IoT. Negara-negara dan organisasi internasional akan semakin memahami pentingnya keamanan dan privasi dalam IoT, dan ini kemungkinan akan berdampak pada hukum dan kebijakan. Standar keamanan yang lebih tinggi akan diperkenalkan dan penegakan hukum yang lebih ketat terhadap pelanggaran kemungkinan akan terjadi.

8.7 Kesimpulan

Keamanan dan privasi dalam *Internet of Things* (IoT) telah menjadi topik yang semakin penting dalam era transformasi digital. Sebagai jaringan luas yang menghubungkan perangkat dan sistem di seluruh dunia, IoT membawa potensi yang luar biasa untuk efisiensi dan inovasi, tetapi juga tantangan yang signifikan dalam hal keamanan dan privasi data. Dengan jutaan, bahkan miliaran, perangkat yang terhubung ke jaringan, penting untuk memahami dan mengatasi tantangan-tantangan ini. Seiring dengan semakin banyaknya informasi dan data yang dikumpulkan, disimpan, dan diproses oleh perangkat IoT, kebutuhan untuk prinsip-prinsip seperti Keamanan Berdasarkan Desain (*Security by Design*), Minimalisasi Data, dan Transparansi menjadi semakin mendesak.

Strategi dan teknologi untuk mengamankan IoT melibatkan berbagai pendekatan dan mekanisme, termasuk proteksi jaringan dan sistem, manajemen identitas dan akses, dan penggunaan teknologi kriptografi. Masing-masing elemen ini memainkan peran penting dalam menjaga integritas dan privasi data dalam IoT. Namun, meski berbagai solusi telah dikembangkan dan diimplementasikan, tantangan dalam prakteknya tetap ada, terutama karena skala dan kompleksitas IoT.

Regulasi dan standar juga memainkan peran penting dalam memastikan keamanan dan privasi dalam IoT. Beberapa regulasi telah diperkenalkan di berbagai yurisdiksi untuk mengatasi masalah ini, namun implementasinya dapat memberikan tantangan tersendiri. Standar keamanan IoT juga telah dikembangkan dan diperbarui secara berkelanjutan untuk menjaga langkah dengan perkembangan teknologi. Meskipun penting, tantangan dalam implementasi dan kepatuhan terhadap regulasi dan standar ini dapat menghambat efektivitasnya.

Di masa depan, tantangan ini akan terus ada dan berkembang seiring dengan pertumbuhan dan perkembangan IoT. Solusi yang telah dikembangkan dan yang akan datang akan perlu

diadaptasi dan ditingkatkan untuk menjaga langkah dengan perubahan ini. Dengan memahami dan menerapkan prinsip-prinsip keamanan dan privasi, dan dengan melibatkan strategi dan teknologi yang tepat, kita dapat bergerak maju dalam transformasi digital, memahami dan merangkul IoT, sambil menjaga keamanan dan privasi data yang sangat penting.

Sebagai penutup, penting untuk diingat bahwa keamanan dan privasi dalam IoT bukanlah tugas yang mudah. Tetapi dengan kerja keras, dedikasi, dan pengetahuan yang tepat, kita dapat memastikan bahwa transformasi digital yang sedang berlangsung bisa berjalan dengan baik dan aman. Semua pihak, mulai dari perancang perangkat dan sistem, regulator, hingga pengguna akhir, memiliki peran penting dalam mencapai tujuan ini. Dengan bekerja sama, kita dapat memanfaatkan manfaat luar biasa dari IoT sambil menjaga keamanan dan privasi data kita.

DAFTAR PUSTAKA

- Ahmad, I. *et al.* 2018. 'Overview of 5G Security Challenges and Solutions', *IEEE Communications Standards Magazine*, 2(1), pp. 36–43. Available at: <https://doi.org/10.1109/MCOMSTD.2018.1700063>.
- Al-Fuqaha, A. *et al.* 2015. 'Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications', *IEEE Communications Surveys & Tutorials*, 17(4), pp. 2347–2376. Available at: <https://doi.org/10.1109/COMST.2015.2444095>.
- Alaba, F.A. *et al.* 2017. 'Internet of Things security: A survey', *Journal of Network and Computer Applications*, 88, pp. 10–28. Available at: <https://doi.org/10.1016/j.jnca.2017.04.002>.
- Alrawais, A. *et al.* 2017. 'Fog Computing for the Internet of Things: Security and Privacy Issues', *IEEE Internet Computing*, 21(2), pp. 34–42. Available at: <https://doi.org/10.1109/MIC.2017.37>.
- Atzori, L., Iera, A. and Morabito, G. 2010. 'The Internet of Things: A survey', *Computer Networks*, 54(15), pp. 2787–2805. Available at: <https://doi.org/10.1016/j.comnet.2010.05.010>.
- Bonomi, F. *et al.* 2012. 'Fog computing and its role in the internet of things', in *Proceedings of the first edition of the MCC workshop on Mobile cloud computing*. New York, NY, USA: ACM, pp. 13–16. Available at: <https://doi.org/10.1145/2342509.2342513>.
- Cisco. 2020. *Cisco Annual Internet Report (2018–2023) White Paper*.
- European Data Protection Board. 2019. *Guidelines on Data Minimization*.

- Greenleaf, G. 2017. 'Global Data Privacy Laws 2017: 120 National Data Privacy Laws, Including Indonesia and Turkey', *UNSW Law Research Paper* [Preprint], (No. 17-45).
- Halim, D.K. and Hutagalung, S. 2022. 'Towards data sharing economy on Internet of Things: a semantic for telemetry data', *Journal of Big Data*, 9(1), p. 1. Available at: <https://doi.org/10.1186/s40537-021-00549-0>.
- Jordan. 2019. *SECURE BY DESIGN: CYBERSECURITY AND INTERNET OF THINGS*. Available at: <https://www.cybersecuritycloudexpo.com/2019/12/news/secure-by-design-cybersecurity-and-internet-of-things/> (Accessed: 7 July 2023).
- Kolias, C. *et al.* 2017. 'DDoS in the IoT: Mirai and Other Botnets', *Computer*, 50(7), pp. 80–84. Available at: <https://doi.org/10.1109/MC.2017.201>.
- Kruse, C.S. *et al.* 2017. 'Cybersecurity in healthcare: A systematic review of modern threats and trends', *Technology and Health Care*, 25(1), pp. 1–10. Available at: <https://doi.org/10.3233/THC-161263>.
- Makhdoom, I. *et al.* 2019. 'Anatomy of Threats to the Internet of Things', *IEEE Communications Surveys & Tutorials*, 21(2), pp. 1636–1675. Available at: <https://doi.org/10.1109/COMST.2018.2874978>.
- Miorandi, D. *et al.* 2012. 'Internet of things: Vision, applications and research challenges', *Ad Hoc Networks*, 10(7), pp. 1497–1516. Available at: <https://doi.org/10.1016/j.adhoc.2012.02.016>.
- Mosenia, A. and Jha, N.K. 2017. 'A Comprehensive Study of Security of Internet-of-Things', *IEEE Transactions on Emerging Topics in Computing*, 5(4), pp. 586–602. Available at: <https://doi.org/10.1109/TETC.2016.2606384>.
- Roman, R., Najera, P. and Lopez, J. 2011. 'Securing the Internet of Things', *Computer*, 44(9), pp. 51–58. Available at: <https://doi.org/10.1109/MC.2011.291>.

- SathishKumar, J. and R. Patel, D. 2014. 'A Survey on Internet of Things: Security and Privacy Issues', *International Journal of Computer Applications*, 90(11), pp. 20–26. Available at: <https://doi.org/10.5120/15764-4454>.
- Shieh, S. 2014. 'IoT Security: Ongoing Challenges and Research Opportunities', in *IEEE International Workshop on Internet of Things Services*.
- Sicari, S. *et al.* 2015. 'Security, privacy and trust in Internet of Things: The road ahead', *Computer Networks*, 76, pp. 146–164. Available at: <https://doi.org/10.1016/j.comnet.2014.11.008>.
- Standaert, F.-X. 2010. 'Introduction to Side-Channel Attacks', in, pp. 27–42. Available at: https://doi.org/10.1007/978-0-387-71829-3_2.
- Symantec. 2019. *2019 Symantec Internet Security Threat Report*.
- Wang, A.B. 2016. *Can Alexa help solve a murder? Police think so — but Amazon won't give up her data*. Available at: <https://www.washingtonpost.com/news/the-switch/wp/2016/12/28/can-alexa-help-solve-a-murder-police-think-so-but-amazon-wont-give-up-her-data/> (Accessed: 7 July 2023).
- Weber, R.H. 2010. 'Internet of Things – New security and privacy challenges', *Computer Law & Security Review*, 26(1), pp. 23–30. Available at: <https://doi.org/10.1016/j.clsr.2009.11.008>.
- Widjaja, M., Halim, D.K. and Andarini, R. 2022. 'The Development of an IoT-based Indoor Air Monitoring System Towards Smart Energy Efficient Classroom', *Ultima Computing: Jurnal Sistem Komputer*, pp. 28–35. Available at: <https://doi.org/10.31937/sk.v14i1.2565>.
- Xiao, L. *et al.* 2018. 'IoT Security Techniques Based on Machine Learning: How Do IoT Devices Use AI to Enhance Security?', *IEEE Signal Processing Magazine*, 35(5), pp. 41–49. Available at: <https://doi.org/10.1109/MSP.2018.2825478>.

Zarpelão, B.B. *et al.* 2017. 'A survey of intrusion detection in Internet of Things', *Journal of Network and Computer Applications*, 84, pp. 25–37. Available at: <https://doi.org/10.1016/j.jnca.2017.02.009>.

BAB 9

INTERNET OF THINGS DAN TRANSPORTASI MASA DEPAN

Oleh Rudi Sutomo

9.1 Introduction



Gambar 10.1. IoT Sektor Transportasi
(Sumber : www.freepik.com)

Konsep "*Internet of Things*" (IoT) mengacu pada perangkat yang terhubung ke internet dan dilengkapi dengan teknologi seperti sensor dan software dengan tujuan untuk berkomunikasi, mengendalikan, menghubungkan, dan bertukar data dengan perangkat lain. AI (kecerdasan buatan), sensor, dan konektivitas membentuk ekosistem *Internet of Things*. Akibatnya, sensor yang

memungkinkan *Internet of Things* untuk mengintegrasikan perangkat memungkinkan komunikasi *real-time* antar perangkat tanpa intervensi manusia. *Internet of Things* (IoT) digunakan dalam banyak industri, salah satunya adalah sektor transportasi. Industri ini menggunakan teknologi *Internet of Things* untuk mengontrol, mengumpulkan data, dan mengintegrasikan sistem transportasi. Berbagai mesin kendaraan melihat pengembangan *Internet of things* yang cepat di sektor ini. Ini juga merupakan cara IOT bekerja di sektor transportasi.

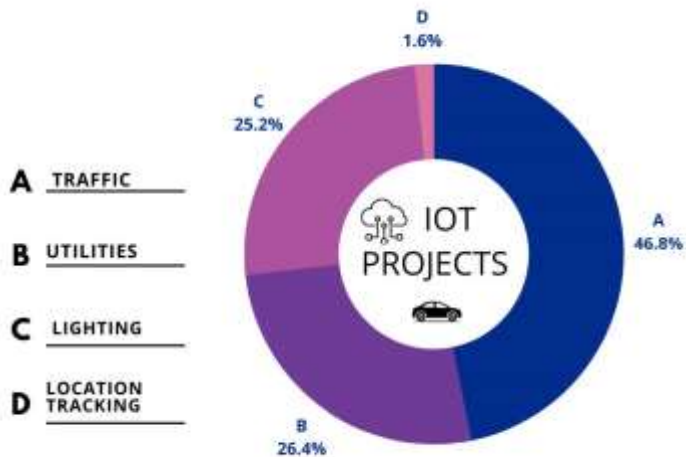
Aplikasi transportasi pintar generasi berikutnya muncul sebagai hasil dari kemajuan baru dalam jaringan sensor nirkabel, komputasi awan, data besar, dan *Internet of Things* (IoT). *Internet of Things* terdiri dari jaringan objek fisik berkemampuan web yang memiliki perangkat keras komunikasi, prosesor, dan sensor yang mengumpulkan data dari lingkungannya. Sebagai dasar sistem transportasi pintar, perangkat ini berfungsi sebagai platform pemantauan luas yang memungkinkan pengumpulan dan pertukaran data dalam jumlah besar secara *real-time*.

Dengan menggabungkan teknologi dan implikasi sosial, *Internet of Things* adalah penemuan yang dapat memecahkan masalah saat ini. Ini adalah sistem yang tersebar di seluruh dunia yang memenuhi tuntutan masyarakat. Perkembangan TIK saat ini dan masa depan memungkinkan layanan lanjutan dengan koneksi fisik dan virtual. Sesuai namanya, *Internet of Things* mengacu pada penggabungan data dari berbagai jenis objek ke platform virtual apa pun dengan infrastruktur *Internet* yang ada saat ini.

Beberapa komponen transportasi pintar memiliki aplikasi *Internet of Things* (IoT) yang telah berkembang. Lalu lintas cerdas, parkir cerdas, dan mobilitas cerdas adalah contohnya. Transportasi pintar saat ini dapat menawarkan banyak fitur, termasuk pemesanan parkir cepat, penerangan jalan yang ekonomis, telematika untuk transportasi umum, penghindaran kecelakaan, dan pengemudi otonom menggunakan sensor yang terintegrasi

dalam mobil atau perangkat seluler dan perangkat yang digunakan di kota.

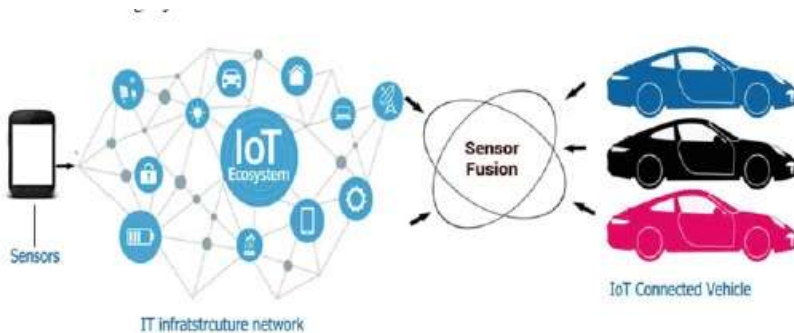
Analitis *Internet of Things* menunjukkan peningkatan penggunaan *Internet of Things* di berbagai sektor transportasi. Pengaturan manufaktur/industri adalah yang paling populer pada 22%, diikuti oleh proyek transportasi/mobilitas pada 15%, dan energi IoT pada 14%, menurut penelitian yang dilakukan pada tahun 2020 tentang kategori aplikasi IoT teratas [61]. Menurut penelitian mereka, penggunaan *Internet of Things* (IoT) paling banyak dilakukan oleh sektor transportasi dalam berbagai proyek. Jumlah proyek yang memanfaatkan Internet of Things untuk menyediakan solusi transportasi ditunjukkan pada Gambar 9.2 (Oladimeji *et al.*, 2023).



Gambar 9.2. Proyek transportasi IoT berdasarkan segmen pada tahun 2020.

(Sumber : *Smart Transportation: An Overview of Technologies and Applications*, (Oladimeji *et al.*, 2023)

Mobilitas pintar mengacu pada kendaraan pintar, mobil berdasarkan penggunaan aktivitas sehari-hari di kota pintar (seperti Gambar 9.2). Transportasi data perkotaan (meliputi mobil, taksi, bus, dan kereta api), yang perlu menggabungkan data dalam jaringan transportasi dan mobil berbagi jaringan. Mobilitas Cerdas adalah alat yang berguna untuk mencapai masa depan yang lebih potensial. Efek mobilitas pintar pada struktur layanan mobil. Dua istilah penting untuk menginformasikan *Vehicle-to-vehicle* dan kendaraan-ke-infrastruktur. Teknologi *Vehicle-to-vehicle* (V2V) adalah komunikasi antara dua atau lebih kendaraan. Teknologi kendaraan terhubung secara infrastruktur (V2I) adalah sebuah koneksi terpusat antara kendaraan dan infrastruktur yang digunakan untuk pengiriman informasi secara bersamaan ke infrastruktur. Mobilitas Cerdas adalah sangat luas visi, dan penelitian Mobilitas Cerdas masih dalam tahap awal. Mobilitas Cerdas didefinisikan dengan “penggunaan data dan Komunikasi Teknologi dalam teknologi transportasi baru untuk meningkatkan lalu lintas perkotaan”. Mobilitas Cerdas “adalah gagasan tentang masa depan yang komprehensif dan lebih cerdas.” (Doaa,2020).



Gambar 9.3. IoT Sektor Transportasi
(Sumber : *Information Integrity for Multi-sensors*)

Data Fusion in Smart Mobility, Doaa et al, 2020)

Mobilitas Cerdas didefinisikan sebagai "aksesibilitas lokal dan supra-lokal, ketersediaan TIK, sistem transportasi modern, berkelanjutan dan aman." Dalam domain transportasi dan mobilitas cerdas, ada banyak taksonomi kota pintar, termasuk taksonomi klasifikasi untuk kota pintar yang menggambarkan model bisnis; informasi tentang mobilitas dan penumpang mobilitas; dan taksonomi kota pintar lainnya. Di sana ada taksonomi mobilitas yang cerdas. Penelitian tentang mobilitas pintar yang menjaga integritas data fusi multisensor diusulkan kepada kami. Infrastruktur yang efektif untuk menurunkan biaya sistem lampu lalu lintas GPS mengumpulkan lokasi ponsel pengendara sepeda, arah, dan kecepatan. layanan lalu lintas yang dikombinasikan dengan teknologi internet of things yang cerdas. Mobilitas cerdas masyarakat dianggap sebagai model sistem manajemen kendaraan dan komunikasi dalam sistem mengikuti lalu lintas cerdas.(Doaa,2020).

9.2 Benefits of the IoT in Transportation



Gambar 9.4. Ilustrasi Benefit IoT Transportasi
(Sumber : www.freepik.com)

9.2.1 Meningkatkan Efisiensi

Teknologi *Internet of Things* (IoT) dapat digunakan untuk mengoptimalkan proses transportasi, yang dapat meningkatkan efisiensi dalam hal waktu dan biaya. Dengan mengumpulkan data dan informasi secara real-time, pengguna dapat membuat keputusan yang lebih tepat tentang rute dan kendaraan yang tepat, sehingga dapat menghindari kemacetan dan menghemat waktu. Selain itu, teknologi IoT dapat membantu mengoptimalkan penggunaan bahan bakar, sehingga dapat menghemat lebih banyak bahan bakar.

9.2.2 Meningkatkan Keamanan

Teknologi *Internet of Things* (IoT) dapat meningkatkan keamanan transportasi dengan menempatkan sensor di kendaraan yang memantau kinerja kendaraan dan memberikan informasi yang diperlukan untuk mencegah kerusakan atau kecelakaan. Selain itu, teknologi IoT juga dapat digunakan untuk memantau lalu lintas dan memberikan informasi kemacetan dan kecelakaan secara real-time, sehingga pengguna dapat mengambil tindakan yang tepat untuk mencegah kecelakaan.



Gambar 9.5. Ilustrasi Security pada IoT Kendaraan
(Sumber : www.freepik.com)

9.2.3 Mengurangi Emisi

Teknologi *Internet of Things* (IoT) memungkinkan pengguna untuk mengurangi emisi gas rumah kaca dengan menganalisis kinerja kendaraan dan mengoptimalkan penggunaan bahan bakar, sehingga mengurangi emisi gas rumah kaca.

9.2.4 Meningkatkan Pengalaman Pengguna

Jaringan transportasi pintar yang menggunakan teknologi IoT dalam transportasi dapat membantu meningkatkan pengalaman pengguna. Dengan memberikan informasi *real-time* tentang lalu lintas serta keadaan jalan, pengguna dapat memilih rute alternatif yang lebih cepat dan menghemat waktu. Selain itu, teknologi IoT juga dapat membantu dalam pembayaran otomatis, sehingga pengguna dapat membeli tiket transportasi dengan mudah dan cepat.

9.2.5 Meningkatkan Manajemen Logistik

Dalam hal manajemen logistik, teknologi IoT dapat membantu perusahaan logistik dalam mengoptimalkan rute pengiriman serta meminimalkan risiko kehilangan atau kerusakan barang. Dengan menggunakan sensor serta perangkat terhubung lainnya, informasi dapat diberikan secara *real-time* tentang lokasi, kondisi, serta keamanan barang.

9.3 Self-driving Cars



Gambar 9.6. Ilustrasi Kendaraan Otonom
(Sumber : www.freepik.com)

Konsep "*Internet of Things*" (IoT) mengacu pada perangkat yang terhubung ke internet dan dilengkapi dengan teknologi seperti sensor dan software dengan tujuan untuk berkomunikasi, mengendalikan, menghubungkan, dan bertukar data dengan perangkat lain. AI (kecerdasan buatan), sensor, dan konektivitas membentuk ekosistem *Internet of Things*. Akibatnya, sensor yang memungkinkan *Internet of Things* untuk mengintegrasikan perangkat memungkinkan komunikasi real-time antar perangkat tanpa intervensi manusia. *Internet of Things* (IoT) digunakan dalam banyak industri, salah satunya adalah sektor transportasi. Industri ini menggunakan teknologi *Internet of Things* untuk mengontrol, mengumpulkan data, dan mengintegrasikan sistem transportasi. Berbagai mesin kendaraan melihat pengembangan internet of things yang cepat di sektor ini. Ini juga merupakan cara IOT bekerja di sektor transportasi.

Kendaraan otonom atau *self-driving cars* menggunakan teknologi IoT untuk mengintegrasikan sensor dan sistem penginderaan yang canggih. Hal ini memungkinkan mobil untuk

secara mandiri mengenali lingkungannya, berkomunikasi dengan kendaraan lain, dan mengambil keputusan yang aman dan efisien dalam berkendara. Menurut sebuah artikel terbaru dari IEEE Spectrum, penelitian terus dilakukan untuk meningkatkan kemampuan kendaraan otonom ini dalam beradaptasi dengan berbagai kondisi jalan dan memastikan keamanan penggunaannya (IEEE Spectrum, 2023).

9.4 Smart Charging Station



Gambar 9.7. Penggunaan IoT Pada Stasiun Pengisian Baterai Kendaraan

(Sumber : www.freepik.com)

Dengan mengumpulkan data ketersediaan dan menampilkannya kepada pengguna melalui aplikasi mobile, *Internet of Things* dapat digunakan untuk meningkatkan sistem pengisian baterai kendaraan listrik.

Dengan adanya sistem IoT pada stasiun pengisian daya kendaraan listrik, pengguna dapat memantau dan mengatur pengisian daya melalui aplikasi atau platform terhubung. Ini memungkinkan pengguna untuk mengoptimalkan penggunaan energi, memanfaatkan waktu pengisian secara efisien, dan menghindari pembebanan jaringan listrik secara berlebihan.

Menurut laporan terbaru dari *Deloitte*, pengembangan infrastruktur *smart charging station* yang terhubung secara IoT diharapkan dapat meningkatkan adopsi kendaraan listrik dan memfasilitasi transisi menuju mobilitas yang lebih berkelanjutan (Smith, Sanborn and Slaughter, 2017).

9.5 Smart Parking



Gambar 9.8. Ilustrasi Pada Kendaraan Cerdas
(Sumber : www.freepik.com)

IoT dapat digunakan untuk memperbaiki sistem parkir dengan mengumpulkan data tentang ketersediaan tempat parkir dan kemudian menampilkannya kepada pengguna melalui aplikasi *mobile*. Pengelola parkir juga dapat menggunakan sistem IoT untuk mengetahui di mana slot parkir yang masih kosong. Dengan bantuan sensor jarak dan infra merah, sistem IoT dapat membantu pengelola parkir dan pengguna parkir mengetahui di mana mereka harus memarkir mobil mereka. Kantor perusahaan biasanya terletak di gedung yang juga digunakan oleh kantor perusahaan lain. Salah satu efeknya adalah sulitnya mencari tempat parkir baik

untuk pekerja maupun pengunjung. Padahal, banyak orang merasa mencari tempat parkir menjengkelkan. Smart parking memungkinkan karyawan Anda tidak lagi mencari tempat parkir kosong. Karena itu, tempat parkir akan dilengkapi dengan sensor yang akan mendeteksi ruang parkir kosong dan secara real-time memberikan informasi kepada pengguna melalui aplikasi.

Dengan demikian, karyawan Anda tidak perlu mencari tempat parkir kosong, dan mereka dapat masuk ke kantor lebih cepat dan dengan senang hati. Akhirnya, tingkat kepuasan karyawan meningkat. Tempat parkir pintar menggunakan perangkat terhubung dan sensor untuk mengetahui ketersediaan tempat parkir. Dengan menggunakan aplikasi atau platform yang terintegrasi, pengendara dapat melihat informasi secara real-time tentang tempat parkir yang tersedia di sekitar mereka. Studi terbaru yang diterbitkan dalam jurnal "*IEEE Transactions on Intelligent Transportation Systems*" menyatakan bahwa penggunaan sistem smart parking dapat mengurangi waktu mencari parkir hingga 30%, mengurangi kemacetan, dan emisi karbon di perkotaan (Oladimeji *et al.*, 2023).

9.6 IoT System for Car Safety



Gambar 9.9. Ilustrasi Pada Kendaraan Cerdas
(Sumber : www.freepik.com)

Keamanan dan Efisiensi *Internet of Things* (IoT) adalah teknologi yang digunakan dalam kehidupan sehari-hari dalam berbagai industri, seperti transportasi, dan memungkinkan perangkat terhubung satu sama lain untuk berkomunikasi dan bertukar data melalui jaringan internet. Contoh IoT dalam transportasi meliputi berbagai teknologi yang dapat meningkatkan efisiensi serta keamanan dalam transportasi. Artikel ini akan membahas contoh-contoh IoT dalam transportasi dan bagaimana teknologi ini dapat memberikan manfaat dalam berbagai bidang transportasi.

Misalnya, meskipun kita mendapatkan manfaat langsung dari asuransi atau memiliki mobil baru yang baru saja kita beli, itu masih merupakan hal yang tidak menyenangkan jika mobil baru kita harus dirawat di bengkel untuk perbaikan, bukan? Kita juga tidak tahu apakah asuransi membayar kerusakan kecil pada mobil kita. Untuk mengetahui jangkauan layanan asuransi mereka, Anda dapat memeriksa asuransi mobil terbaik saat ini. Jika mobil tersebut memiliki sistem parkir yang memungkinkan kita memarkir kendaraan kita dengan lebih aman, pasti akan lebih nyaman. Ada beberapa hal yang bekerja dengan alarm sistem parkir mobil ini. Yang pertama adalah sistem tertanam, yang berfungsi sebagai pusat sistem parkir. Selanjutnya ada sensor radar, yang menggunakan sensor jarak jauh, buzzer, dan layar untuk memberikan informasi kepada pengemudi. Sistem alarm yang lebih canggih memiliki kamera belakang yang terintegrasi dengan sensor jarak, dan tampilan LCD di dashboard untuk memudahkan memarkir mobil. Siapa sih yang mau mengalami kerusakan pada kendaraan kesayangannya, meskipun kita dilindungi oleh asuransi? Sudah jelas bahwa tujuan asuransi adalah untuk mengurangi resiko. Namun, dengan teknologi terbaru, kita juga dapat mengurangi resiko.

Sebaliknya, sistem *Internet of Things* dapat berfungsi sebagai pengaman mobil. Dengan menggunakan sistem penguncian IoT seperti *RFID*, *Bluetooth*, atau *WiFi*, mobil hanya

dapat dinyalakan jika pemiliknya terdeteksi berada di dekatnya. Selain itu, sistem IoT akan mengeluarkan alarm jika sensor menemukan upaya untuk membuka pintu mobil secara paksa. Di masa depan, kita akan lebih banyak berinteraksi dengan mobil otonom jika mereka memiliki AI dan dukungan IoT untuk mengemudi sendiri dan menemukan jalan terbaik keluar kemacetan.

Saat ini, banyak mobil yang dioperasikan di gudang di atas yang tidak perlu dikendarai oleh petugas. Kendaraan tersebut dilengkapi dengan sensor yang dapat mendeteksi kondisi sekitar sehingga dapat berjalan secara mandiri tanpa menabrak apa pun. Saat ini, tidak hanya di gudang, banyak individu dan perusahaan yang mengembangkan kendaraan yang dapat bergerak sendiri. Tentu saja, karena banyaknya kendaraan yang bergerak, jalanan umum, terutama di Indonesia, akan jauh lebih menantang untuk kendaraan otomatis. Di tahun 1996, misalnya, komponen yang dikenal sebagai *onboard diagnostic port* (OBDs) telah ditanamkan ke dalam mesin mobil. OBD adalah bagian yang dapat secara otomatis memantau kondisi kesehatan mobil. Karena OBD mengurangi pengecekan manual, pekerjaan mekanik menjadi lebih mudah. Selain itu, pemilik mobil memiliki kemampuan untuk memantau kondisi kendaraan mereka melalui monitor tanpa harus mempelajari banyak tentang permesinan mobil. OBD akan menampilkan peringatan di monitor jika mereka menemukan bahwa mobil Anda mengalami masalah.

Melalui IoT, kendaraan dapat terhubung dengan jaringan sensor yang memantau kondisi mesin, sistem kelistrikan, dan komponen lainnya. Dengan demikian, pemilik atau pengelola armada dapat memperoleh informasi real-time tentang performa dan kebutuhan perawatan kendaraan. Penelitian dari Frost & Sullivan menunjukkan bahwa penerapan solusi smart maintenance melalui IoT dapat mengurangi biaya perawatan hingga 20% dan mengoptimalkan efisiensi bahan bakar, sehingga mengurangi emisi kendaraan (Frost & Sullivan, 2022).



Gambar 9.10. Ilustrasi Efisiensi pada Kendaraan Cerdas
(Sumber : <https://intellias.com/how-can-the-automotive-industry-use-internet-of-things-iot-technology>, Frost & Sullivan, 2022)

Sistem keamanan terkoneksi menggunakan *Internet of Things* untuk meningkatkan keamanan mobil. Kamera dan sensor yang terhubung dengan kendaraan dapat mendeteksi bahaya seperti kecelakaan, pencurian, atau aktivitas mencurigakan di sekitar kendaraan. Sebuah studi dari "*International Journal of Distributed Sensor Networks*" menemukan bahwa sistem keamanan IoT pada kendaraan dapat meningkatkan keselamatan pengemudi, mengurangi tingkat kejahatan terkait mobil, dan mengurangi risiko kehilangan kendaraan (Sabri, Siham and Maizate, 2021).

9.7 Smart Public Transport

Dengan melacak posisi bus dan kereta api, dan memberi pengguna aplikasi mobile, IoT dapat membantu mengoptimalkan sistem transportasi umum. Contoh di atas menunjukkan penggunaan teknologi internet pada bus Seoul. Ini adalah salah satu contoh aplikasi Internet of Things dalam kota pintar. Data tentang jumlah penumpang dan lokasi kendaraan akan dikirim

melalui sensor yang dipasang di setiap bus dan halte. Selanjutnya, data akan dikirim secara real-time melalui aplikasi yang digunakan penumpang dan panel yang ada di setiap halte. Dengan demikian, pengguna transportasi publik lebih puas. Pada akhirnya, harapannya adalah kemacetan akan berkurang karena semakin banyak orang yang menggunakan transportasi publik. Dengan data real-time dari aplikasi, efisiensi penggunaan transportasi publik untuk berbagai kebutuhan dapat ditingkatkan. Dengan peningkatan efisiensi ini, diharapkan masyarakat lebih suka menggunakan kendaraan publik dan meninggalkan kendaraan pribadi. Beralih dari kendaraan pribadi ke kendaraan umum akan mengurangi kemacetan. Bagi pebisnis, mengurangi kemacetan sama dengan bertemu dengan klien secara tepat waktu dan memiliki karyawan yang datang ke tempat kerja dengan senyuman dan tepat waktu.



Gambar 9.11. Ilustrasi Pada Kendaraan Cerdas
(Sumber : www.freepik.com)

Dengan penerapan teknologi IoT, manajemen transportasi publik menjadi lebih efisien dan adaptif. Melalui sensor dan analisis data real-time, sistem *smart public transport* dapat mengoptimalkan rute, jadwal, dan kapasitas kendaraan untuk mengakomodasi kebutuhan penumpang. Selain itu, dengan adanya aplikasi ride-sharing yang terhubung dengan sistem transportasi publik, pengguna dapat dengan mudah mencari dan memanfaatkan layanan transportasi yang berbagi. Sebuah penelitian yang diterbitkan dalam jurnal "*Transportation Research Part C: Emerging Technologies*" menyebutkan bahwa penggunaan IoT dalam manajemen transportasi publik dapat membantu meminimalisir kecelakaan lalu lintas, mengurangi waktu perjalanan, dan meningkatkan efisiensi penggunaan infrastruktur transportasi (Oladimeji et al, 2023).



Gambar 9.12. Iot Pada Penggunaan Transportasi Umum Cerdas
(Sumber : www.freepik.com)

9.8 Vehicle Tracking Systems

IoT dapat melacak lokasi kendaraan dan mengumpulkan data seperti kecepatan, jarak tempuh, dan kondisi kendaraan, yang dapat digunakan untuk meningkatkan efisiensi dan mengurangi biaya. Teknologi *Internet of Things* (IoT), khususnya sistem pengejaran kendaraan, sangat bermanfaat untuk kelancaran proses manajemen rantai pasokan perusahaan Anda, baik menggunakan armada Anda sendiri maupun armada mitra. Secara sederhana, Anda dapat melacak lokasi kendaraan yang digunakan supplier untuk mengirimkan bahan baku kepada Anda dan lokasi armada yang Anda gunakan untuk mengirimkan produk ke gudang, cabang, atau pelanggan.



Gambar 9.13. Ilustrasi Pelacakan Pada Kendaraan
(Sumber : www.freepik.com)

Selain itu, Anda dapat membuat jadwal keberangkatan armada, mengetahui waktu rata-rata pengiriman barang, jumlah bahan bakar yang dibutuhkan, sopir dan kondektur yang ditugaskan, dan informasi lainnya. Akibatnya, Anda dapat meningkatkan efisiensi dan efektivitas proses rantai pasokan bisnis Anda. Semakin besar bisnis Anda, semakin banyak bahan baku yang harus Anda beli dari supplier dan produk yang harus Anda

kirim ke cabang, gudang lokal, toko, dan konsumen akhir. Penggunaan teknologi *Internet of Things* (IoT) di sektor ini meningkatkan efisiensi dan produktivitas rantai pasokan. karena Anda dapat mengetahui banyak informasi penting tentang rantai pasokan tanpa harus terjun langsung ke lapangan. Mobil otomatis dapat menggantikan tenaga kerja manusia yang tidak efisien, bahkan jika teknologi kendaraan pribadi sudah dapat digunakan untuk kendaraan komersial jarak jauh.

Untuk mengelola kendaraan bermotor perusahaan, seperti motor, mobil, dan bus, sistem pengelolaan flotasi adalah salah satu sistem yang dikembangkan. Hasilnya adalah Anda dapat memaksimalkan pemanfaatan kendaraan Anda, menghemat bahan bakar perusahaan, dan memprediksi waktu pemeliharaan yang lebih lama untuk mobil Anda. Fleet management dilakukan dengan tujuan meningkatkan efisiensi dan produktivitas serta meningkatkan keselamatan pengemudi dan pengendara. Tujuan ini memerlukan kombinasi sistem yang dapat memantau kebiasaan driver, melacak lokasi kendaraan perusahaan, melaporkan penggunaan bahan bakar, dan mengelola pemeliharaan kendaraan. Software GPS yang semakin canggih sekarang dapat membantu setiap pengemudi menemukan rute terbaik untuk perjalanan mereka. Fitur ini dapat membantu pengemudi dalam pekerjaan mereka dan mengurangi risiko tersesat atau salah jalur. Bahan bakar secara otomatis terbuang ketika pengemudi harus memutar arah karena salah mengambil jalur. Selain itu, tingkat kemacetan akan berdampak pada waktu pengiriman dan kualitas produk. Dengan adanya penunjuk jalan dan pelacak pengemudi, yang juga dikenal sebagai "*route optimization*", efek yang paling signifikan dari fitur ini adalah jarak waktu tempuh yang lebih sedikit, yang berarti lebih sedikit bahan bakar yang digunakan. Meskipun terlihat mudah, melacak empat kendaraan yang membawa lima belas sepeda motor jelas merupakan tugas yang sulit. Teknologi GPS dan sistem pelacakan sistem manajemen kapal

memungkinkan Anda mengetahui dengan lebih akurat di mana pengemudi berhenti atau tersesat.

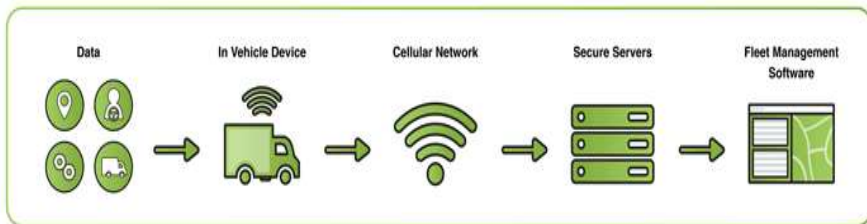


Gambar 9.14. Iot Pada Pengaturan GPS pada Kendaraan Cerdas
(Sumber : www.freepik.com)

Contoh berikut menunjukkan bahwa semua kendaraan bermotor memerlukan bahan bakar untuk menghitung pemakaian bahan bakar yang diprediksi. Sepertiga dari biaya operasional kendaraan ditanggung oleh bahan bakar. Untuk alasan ini, pengisian bahan bakar harus diperhatikan. Meskipun kelebihan biaya bahan bakar ini kecil, namun jika dijumlahkan setiap bulan, itu pasti akan mengurangi keuntungan bisnis. Manajemen penggunaan bahan bakar yang tidak teratur pasti akan berdampak buruk dan mengancam kelancaran operasi. Jadi, fitur yang mengantisipasi konsumsi bahan bakar dapat membantu Anda menghitung banyaknya biaya bahan bakar yang diperlukan untuk setiap jenis kendaraan.

Sejak beberapa tahun terakhir semenjak revolusi industri kemajuan bisnis di dunia nyaris dipengaruhi dengan bantuan IoT. Berbagai bidang bisnis melesat dengan cepat dengan adanya bantuan IoT, salah satunya di sektor transportasi. Kebutuhan

berpindah dari satu tempat ke tempat lain membutuhkan efisiensi agar bisa sampai ke tujuan dengan cepat. Jika Anda adalah pelaku bisnis yang menggunakan banyak armada kendaraan dalam operasionalnya, salah satu sistem untuk mengoptimalkan kegiatan bisnis adalah *fleet management system*.



Gambar 9.15. IoT dalam Transportasi Logistik

(Sumber : <https://www.teletracnavman.com/fleet-management-software/telematics/resources/iot-in-transportation-logistics-the-ultimate-guide>)

Sistem pengelolaan kendaraan juga dapat melacak kecepatan kendaraan, pengereman mendadak, dan akselerasi yang sangat cepat. Pada akhirnya, sistem ini akan secara otomatis melaporkan seluruh kondisi, memungkinkan perusahaan untuk melakukan evaluasi manajemen dan audit perilaku pengemudi. Sistem manajemen kendaraan juga memiliki fitur untuk mengingatkan waktu service kendaraan. Kendaraan biasanya memerlukan waktu yang lebih lama untuk menguji kinerja mesin. Agar Anda tidak lupa tentang waktu pemeliharaan yang sudah semakin dekat, alarm akan dibunyikan oleh sistem manajemen truk. Sistem ini tidak hanya melakukan pekerjaan rutin, tetapi juga akan mengingatkan Anda tentang waktunya untuk mengganti oli. Dengan demikian, usia kendaraan bertambah. Dengan mengelola fleet management, Anda dapat mengurangi biaya total dan perawatan kendaraan. Untuk menciptakan operasi bisnis yang lebih efisien, manajemen kapal akan mengidentifikasi, merinci, dan mengurangi pengeluaran

yang tidak diperlukan. Biaya operasional dan perawatan kendaraan akan terus meningkat, tetapi dengan memulai pelacakan aset dan program efisiensi yang lebih awal, Anda pasti akan melihat peningkatan persentase produktivitas perusahaan Anda.



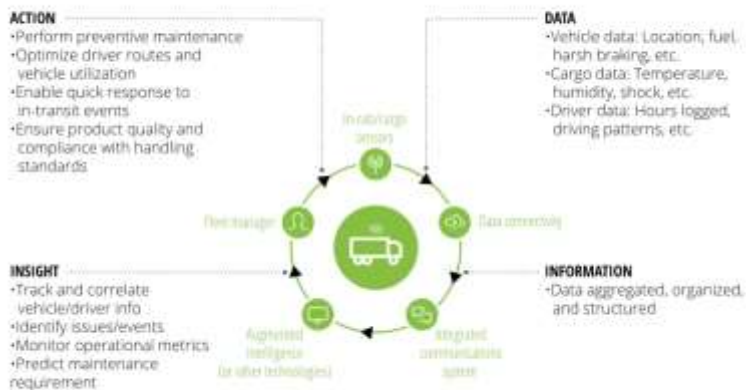
Gambar 9.16. Ilustrasi Iot Pada Pengaturan GPS pada Kendaraan Logistik Cerdas
(Sumber : www.freepik.com)

Model persewaan mobil masa depan adalah contoh tambahan yang dapat kita gunakan untuk memahami istilah *Ride-sharing*. Salah satu contohnya adalah *Car2Go*, layanan *ride-sharing* yang sangat terkenal di Eropa. Layanan ini menggunakan pendekatan kerja yang sangat bergantung pada transportasi *Internet of Things*. Dalam wilayah tertentu, penyedia layanan akan memungkinkan pelanggan menyewa mobil. Smartphone memberi pengguna kemampuan untuk mengontrol akses. Setelah itu, penyedia layanan akan melacak lokasi untuk memantau ke mana Anda membawa mobil tersebut. Penyedia harus memantau lokasi selain lokasi baterai. Memarkir kendaraan di jalan raya seringkali

membingungkan, memperkirakan jarak tempuh berdasarkan bahan bakar seringkali salah, dan pengemudi seringkali membutuhkan pengereman otomatis untuk memenuhi berbagai kebutuhan transportasi lainnya. Ini semua dapat dicapai ketika implementasi internet of things dalam kendaraan dilakukan.

FIGURE 2

Information flow in the transportation ecosystem¹⁴



Source: Deloitte analysis.

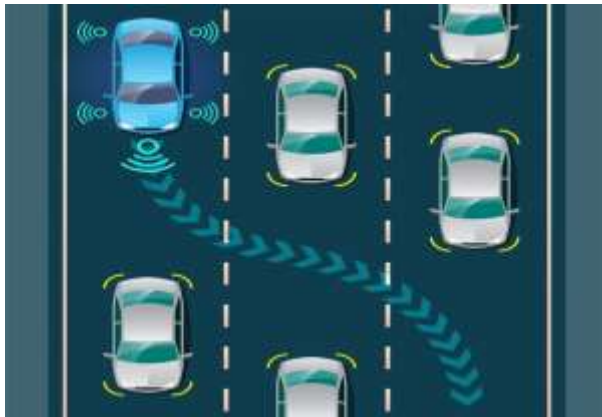
Deloitte insights | deloitte.com/insights

Gambar 9.17. Alur Informasi IoT pada Transportasi

(Sumber : <https://www.teletracnavman.com/fleet-management-software/telematics/resources/iot-in-transportation-logistics-the-ultimate-guide>)

Melalui sistem IoT, pengelola armada dapat melacak dan memantau kendaraan secara real-time. Sensor dan perangkat terhubung pada kendaraan memungkinkan pengumpulan data mengenai posisi, kecepatan, kondisi, dan konsumsi bahan bakar. Hal ini membantu dalam manajemen armada yang efisien, pemeliharaan terjadwal, dan pemantauan penggunaan yang optimal. (Praditya, Widhyaestoeti and Pramuko, 2021).

9.9 Smart Traffic Management



Gambar 9.18. Sensor IoT Pada Smart Manajemen *Traffic*
(Sumber : www.freepik.com)

Dengan mengumpulkan data lalu lintas, sensor *Internet of Things* dapat mengubah waktu lampu lalu lintas dan jalan raya untuk mengurangi kemacetan. Dalam konsep *smart city*, sistem IoT juga digunakan untuk mengontrol lalu lintas. Mereka mendeteksi titik-titik yang mengalami jam lalu lintas dan memberi tahu dinas terkait untuk melakukan rekayasa lalu lintas. Dengan kemampuan yang sangat bermanfaat dan perangkat yang sangat ringkas, *Internet of Things* (IoT) memiliki kemampuan untuk membantu mengelola lalu lintas dan mengurangi kemacetan di kota-kota besar. Sehingga lebih hemat daya, sistem *Internet of Things* hanya membutuhkan jumlah arus yang kecil. Saat ini, di beberapa lokasi lalu lintas, NTMC Polri memiliki kamera CCTV yang terintegrasi dengan jaringan NTMC milik Polri. Kamera ini digunakan untuk memantau lalu lintas, mengidentifikasi pelanggaran lalu lintas, dan memberikan teguran kepada pengendara serta menerapkan tilang elektronik. Di masa depan, manfaat IoT akan jauh lebih besar. Saat sebuah kecelakaan terekam oleh sistem CCTV IoT, sistem dapat

dengan cepat menghubungi polisi, ambulance, rumah sakit, jasa marga, dan memperkirakan identitas korban berdasarkan nomor mobil. Di masa depan, rumah sakit dan asuransi mungkin sudah siap membayar korban kecelakaan setelah kecelakaan. Pengendalian lalu lintas yang lebih baik adalah salah satu fungsi Internet of Things dalam sektor transportasi. IoT sangat penting dalam hal ini, terutama pada tahun 2023. Bagaimana itu berfungsi? Sistem saat ini dapat menggunakan rekaman CCTV untuk mengirimkan laporan lalu lintas. Selanjutnya, sistem ini mencakup fitur seperti lampu lalu lintas, parkir pintar, dan bantuan cerdas untuk kecelakaan jalan. Pengguna jalan biasanya tetap akan menghadapi kondisi jalan yang tidak menyenangkan saat melaju di jalan raya yang bebas macet. Ini terutama berlaku saat melewati pintu tol. Pasalnya, kendala tiket menyebabkan banyak kendaraan antri. Setelah mengetahui situasi tersebut, *Internet of Things* menghasilkan inovasi yang sangat berbeda. Di sini, *internet of things* (IoT) mendeteksi mobil bahkan 1 km sebelum pintu masuk, membuat pintu tol lebih responsif dan membiarkan kendaraan melintas setelah membayar. Selain itu, berbagai sistem pembayaran dapat digunakan, termasuk pembayaran digital.



Gambar 9.19. IoT Pendeteksian kendaraan masuk Tol
(Sumber : www.freepik.com)

Dengan penerapan sistem IoT dalam pengaturan lalu lintas, *smart traffic management* dapat memonitor dan mengelola lalu lintas secara efektif. Sensor yang terhubung mengumpulkan data tentang volume kendaraan, kecepatan, dan kepadatan lalu lintas. Dengan analisis data real-time, sistem dapat memberikan informasi kepada pengemudi tentang kondisi lalu lintas yang sedang terjadi dan memberikan pengaturan sinyal lalu lintas yang adaptif. (Wibawa *et al.*, 2022).



Gambar 9.20. IoT Pelacakan Posisi Kendaraan dan Barang
(Sumber : www.freepik.com)

IoT dapat digunakan untuk melacak lokasi barang yang dikirim dan kendaraan. Ini dapat mempercepat pengiriman dan mengurangi biaya. Dengan kendali IoT penuh, industri akan merasakan banyak manfaat logistik dan armada. IoT juga dapat mengawasi kondisi kendaraan dan mencegah masalah di tengah rute. Secara khusus, industri logistik mungkin mendapatkan empat

keuntungan dari penggunaan Internet of Things untuk transportasi, yaitu: melacak pengiriman, mengoptimalkan rute pengiriman, mengurangi biaya logistik yang tidak efisien, dan meningkatkan keuntungan.

Dalam konteks logistik armada, IoT digunakan untuk meningkatkan efisiensi operasional dan pengiriman barang. Melalui sensor dan konektivitas yang terintegrasi, pemilik armada dapat melacak posisi dan kondisi barang secara real-time, memantau suhu dan kelembaban dalam pengiriman, serta mengoptimalkan rute dan jadwal pengiriman. Menurut laporan terbaru dari *Grand View Research*, implementasi solusi smart logistics dengan IoT di industri logistik diperkirakan akan terus berkembang untuk mempercepat proses pengiriman, mengurangi biaya logistik, dan meningkatkan kepuasan pelanggan.(Oladimeji *et al.*, 2023)



Gambar 9.21. Smart logistik Pengiriman Barang via Drone
(Sumber : www.freepik.com)

Smart logistik pengiriman barang menggunakan drone telah menjadi salah satu inovasi yang menjanjikan dalam industri logistik. Drones atau pesawat tanpa awak yang dikendalikan secara

otomatis dapat digunakan untuk mengirimkan paket dengan cepat dan efisien, mengatasi kendala geografis dan lalu lintas jalan yang dapat memperlambat proses pengiriman konvensional. Drones yang terhubung dengan sistem IoT dapat memantau posisi dan status pengiriman secara real-time, memberikan pembaruan yang akurat kepada pelanggan dan pemilik bisnis.

Sebagai contoh, program pengiriman *drone Amazon Prime Air* dikembangkan oleh perusahaan e-commerce Amazon dan menggunakan drone pintar yang dapat mengirimkan paket dengan berat hingga 2,3 kilogram dalam waktu kurang dari tiga puluh menit. Drones yang dilengkapi dengan sensor dan kamera dapat mendeteksi hambatan di sekitarnya, menghindari penghalang, dan secara otomatis mendarat dengan aman. Pengiriman menggunakan drone ini telah diuji coba dan diterapkan dalam beberapa daerah terpilih, seperti di Inggris dan Amerika Serikat, dengan tujuan meningkatkan efisiensi pengiriman dan mempercepat waktu penerimaan barang oleh pelanggan (Benarbia and Kyamakya, 2022).

DAFTAR PUSTAKA

- Doaa Mohey El-Din, Aboul Ella Hassanien and Ehab E. Hassanien.2020.Information Integrity for Multi-sensors Data Fusion in Smart Mobility.
- Shim, Inwook & Choi, Jongwon & Shin, Seunghak & Oh, Tae Hyun & Lee, Unghui & Ahn, Byungtae & Choi, Dong-Geol & Shim, David & Kweon, Inso. 2015. An Autonomous Driving System for Unknown Environments Using a Unified Map. IEEE Transactions on Intelligent Transportation Systems. 16. 1-15. 10.1109/TITS.2015.2389237.
- Frost & Sullivan,2022, The Top Growth Opportunities for IoT in 2023.
- Benarbia, T. and Kyamakya, K. 2022. 'A literature review of drone-based package delivery logistics systems and their implementation feasibility', *Sustainability (Switzerland)*, 14(1), pp. 1–15. Available at: <https://doi.org/10.3390/su14010360>.
- Oladimeji, D. *et al.* 2023. 'Smart Transportation: An Overview of Technologies and Applications', *Sensors*, 23(8), pp. 1–32. Available at: <https://doi.org/10.3390/s23083880>.
- Praditya, F.R., Widhyaestoeti, D. and Pramuko, A.E.K. 2021. 'Kendali Penumpang Otomatis Transportasi Bus Menggunakan Near Field Communication Berbasis Internet of Things', *Jurnal Ilmiah Teknologi Infomasi Terapan*, 7(2), pp. 128–137. Available at: <https://doi.org/10.33197/jitter.vol7.iss2.2021.546>.
- Sabri, Y., Siham, A. and Maizate, A. 2021. 'Internet of Things (IoT) based Smart Vehicle Security and Safety System', *International Journal of Advanced Computer Science and Applications*, 12(4), pp. 708–714. Available at: <https://doi.org/10.14569/IJACSA.2021.0120487>.

- Smith, S., Sanborn, S. and Slaughter, A. 2017. 'The role of electric utilities in the future of mobility', *Deloitte Insights* [Preprint]. Available at: <https://www2.deloitte.com/insights/us/en/focus/future-of-mobility/power-utilities-future-of-electric-vehicles.html>.
- Wibawa, S. *et al.* 2022. 'Perancangan Purwarupa Lampu Lalu Lintas Pintar Untuk Kendaraan Pemadam Kebakaran Menggunakan Internet Of Things', *eProceedings ...*, 1(1), pp. 1–15. Available at: <https://doi.org/10.30865/jurikom.v9i4.4652>.

BAB 10

INTERNET OF THINGS DALAM RUMAH PINTAR

Oleh Risanto Darmawan

10.1 Pendahuluan

Rumah Pintar atau *Smart Home* mengacu pada rumah yang dilengkapi dengan perangkat elektronik dan perangkat lunak yang terhubung ke jaringan internet, yang memungkinkan pengendalian, pengawasan, dan otomatisasi rumah secara cerdas. Salah satu komponen kunci dari Smart Home adalah IoT, yang memungkinkan perangkat-perangkat tersebut saling berkomunikasi dan berinteraksi melalui jaringan internet (Chowdhury, 2017).

IoT merujuk pada jaringan yang terdiri dari perangkat fisik yang terhubung satu sama lain dan ke internet tanpa campur tangan manusia. Dalam konteks Smart Home, perangkat-perangkat ini meliputi lampu pintar, termostat pintar, pengunci pintu pintar, kamera keamanan, peralatan rumah tangga pintar, dan banyak lagi. Setiap perangkat ini dilengkapi dengan kemampuan komunikasi yang memungkinkannya terhubung ke jaringan internet dan berinteraksi dengan perangkat lain. (Yaddarabullah, 2017).

10.2 Ekosistem IoT Smart Home

Dalam ekosistem IoT Smart Home, perangkat-perangkat ini dapat dikendalikan dan dipantau melalui perangkat seluler, tablet, komputer, atau perangkat pengendali lainnya yang terhubung ke internet. Pengguna dapat menggunakan aplikasi khusus, platform

berbasis cloud, atau asisten suara untuk mengendalikan dan memonitor perangkat-perangkat ini dari jarak jauh. (Davies, 2020).

IoT menjadi fondasi yang memungkinkan Smart Home untuk menjadi lebih cerdas, terhubung, dan dapat diatur sesuai keinginan pengguna. Dengan adopsi IoT dalam Smart Home, pengguna dapat merasakan kenyamanan, efisiensi, dan keamanan yang lebih tinggi dalam pengaturan rumah mereka.



Gambar 10.1. IoT Smart Home

(Sumber : www.trakaid.com/how-iot-devices-are-making-home-automation-and-connected-living-a-reality-in-2020)

Cakupan IoT dalam smart home dapat mencakup berbagai aspek, termasuk:

1. Perangkat pintar: Penggunaan perangkat elektronik pintar yang terhubung ke internet, seperti lampu pintar, pengunci pintu pintar, thermostat pintar, kamera keamanan pintar, perangkat rumah tangga pintar (seperti oven, kulkas, atau mesin cuci), pengontrol multimedia, dan lain sebagainya.

2. **Automatisasi rumah:** Integrasi perangkat pintar untuk menciptakan skenario otomatisasi, di mana perangkat berkomunikasi satu sama lain untuk memenuhi kebutuhan dan preferensi penghuni rumah. Misalnya, ketika meninggalkan rumah, sistem otomatisasi dapat mematikan lampu, mengunci pintu, dan menurunkan suhu thermostat.
3. **Monitoring dan keamanan:** Penggunaan sensor pintar dan perangkat keamanan untuk memantau rumah dan memberikan peringatan atau tindakan yang sesuai. Contohnya, sensor gerak dapat mendeteksi kehadiran orang di rumah dan mengaktifkan sistem keamanan atau mengirimkan pemberitahuan ke ponsel penghuni.
4. **Manajemen energi:** Menggunakan solusi IoT untuk mengelola penggunaan energi di rumah dengan lebih efisien. Misalnya, sistem manajemen energi dapat mengoptimalkan penggunaan listrik dengan mematikan perangkat yang tidak digunakan atau menyesuaikan pengaturan suhu untuk mengurangi konsumsi energi.
5. **Kendali jarak jauh:** Kemampuan untuk mengendalikan perangkat pintar dalam rumah secara jarak jauh melalui smartphone, tablet, atau perangkat lain yang terhubung ke internet. Penghuni rumah dapat mengatur pencahayaan, suhu, sistem keamanan, dan perangkat lain bahkan ketika mereka tidak berada di rumah.
6. **Analitik dan pengumpulan data:** IoT dalam smart home juga melibatkan pengumpulan dan analisis data untuk memberikan wawasan yang lebih baik tentang pola penggunaan, kebiasaan, dan preferensi penghuni. Informasi ini dapat digunakan untuk meningkatkan efisiensi energi, mengoptimalkan pengaturan perangkat, atau memberikan rekomendasi yang lebih personal.

Seiring dengan kemajuan teknologi dan munculnya inovasi baru cakupan IoT dalam smart home terus berkembang. Fitur dan

kemampuan tambahan dapat ditambahkan sesuai dengan kebutuhan penghuni rumah dan perkembangan industri IoT.

10.3 Perangkat Pintar

Smart device, juga dikenal sebagai perangkat pintar, merujuk pada perangkat elektronik yang memiliki kemampuan terhubung ke internet dan mampu berinteraksi dengan pengguna dan perangkat lainnya. Perangkat pintar ini biasanya dilengkapi dengan sensor, konektivitas nirkabel, dan kemampuan pengolahan data yang memungkinkannya untuk menjalankan fungsionalitas yang lebih canggih daripada perangkat konvensional (Mada, 2022). Beberapa contoh umum dari smart devices adalah:

1. **Smartphone:** Ponsel pintar adalah salah satu contoh paling umum dari smart device. Selain fitur telepon dan pesan teks, smartphone juga memiliki kemampuan untuk mengakses internet, mengirim email, menjalankan aplikasi, memutar musik dan video, serta melakukan berbagai tugas lainnya.



Gambar 10.2. Smartphone

(Sumber : www.iotworldtoday.com/smart-cities/the-value-chain-is-evolving-for-connected-home-companies)

2. Smart TV: Televisi pintar memiliki konektivitas internet yang memungkinkannya untuk mengakses konten online dan menawarkan berbagai aplikasi dan layanan streaming seperti Netflix, YouTube, atau Spotify. Beberapa smart TV juga dilengkapi dengan asisten suara seperti Google Assistant atau Amazon Alexa untuk memberikan kontrol yang lebih mudah.



Gambar 10.3. SmartTV

(Sumber : techparasol.com/smart-tv-iot-device)

3. Smart Speaker: Speaker pintar seperti Amazon Echo atau Google Home menggunakan asisten suara untuk memberikan respons suara dan melakukan tugas-tugas seperti memainkan musik, memberikan informasi, mengatur alarm, mengendalikan perangkat pintar lainnya, dan masih banyak lagi.



Gambar 10.4. Smart Speaker

(Sumber : beebom.com/lg-thinq-smart-speaker)

4. Smart Watch: Jam tangan pintar dapat menghubungkan pengguna dengan ponsel mereka melalui Bluetooth atau koneksi nirkabel lainnya. Mereka dapat memberikan notifikasi untuk pesan, panggilan telepon, atau email, serta menyediakan berbagai fitur seperti pelacak aktivitas fisik, monitor detak jantung, dan aplikasi kesehatan lainnya.



Gambar 10.5. Smart Watch

(Sumber : www.raypcb.com/smartwatch-iot)

5. Smart Home Appliances: Ini mencakup berbagai perangkat rumah tangga pintar seperti lampu pintar, pengunci pintu pintar, thermostat pintar, oven pintar, kulkas pintar, mesin cuci pintar, dan lain sebagainya. Perangkat ini dapat terhubung ke jaringan rumah pintar dan dikendalikan secara jarak jauh melalui smartphone atau perintah suara.

Kelebihan utama dari smart devices adalah kemampuan mereka untuk terhubung ke internet dan berinteraksi dengan pengguna serta perangkat lainnya. Hal ini memungkinkan pengguna untuk mengontrol dan memantau perangkat mereka dengan lebih mudah dan memberikan akses ke berbagai layanan dan informasi secara online.

10.4 Otomatisasi Rumah

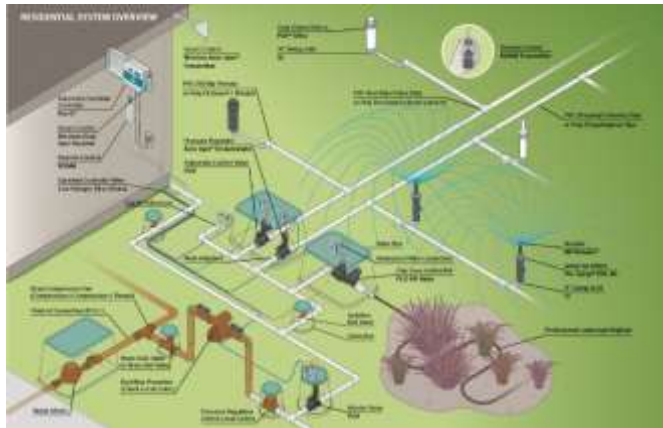
Otomatisasi rumah (*smart home automation*), merujuk pada penggunaan teknologi untuk mengotomatiskan berbagai aspek rumah tangga, termasuk sistem pencahayaan, keamanan, pemanasan dan pendinginan, elektronik konsumen, serta perangkat rumah tangga lainnya. Tujuannya adalah meningkatkan kenyamanan, efisiensi, keamanan, dan kemudahan penggunaan rumah (Kavitha, 2022).

Proses otomatisasi rumah melibatkan penggunaan sensor, perangkat pintar, dan sistem otomatisasi untuk mengumpulkan informasi, mengenali pola, dan mengendalikan perangkat berdasarkan preferensi dan kebutuhan pengguna.

Pencahayaan otomatis, Sensor gerak dapat digunakan untuk mendeteksi kehadiran orang di ruangan dan secara otomatis mengaktifkan atau mematikan lampu. Selain itu, penggunaan sistem pencahayaan terprogram memungkinkan pengaturan pencahayaan yang disesuaikan dengan jadwal atau kegiatan tertentu. Pengunci pintu otomatis, Sistem pengunci pintu pintar dapat diatur untuk mengunci pintu secara otomatis ketika

meninggalkan rumah dan membuka pintu saat mendekati rumah. Hal ini dapat dilakukan melalui pengenalan wajah, kunci digital, atau penggunaan perangkat seluler sebagai kunci pintu. Pengaturan suhu otomatis, Termostat pintar memungkinkan pengguna untuk mengatur jadwal pengaturan suhu yang disesuaikan dengan kebutuhan harian. Sistem ini dapat mempelajari preferensi pengguna dan mengatur suhu secara otomatis berdasarkan jadwal, cuaca, atau kehadiran penghuni rumah. Sistem keamanan otomatis, sistem keamanan rumah pintar menggunakan sensor gerak, kamera keamanan, dan perangkat pendeteksi suara untuk memantau aktivitas dan mendeteksi potensi ancaman. Ketika terdeteksi aktivitas yang mencurigakan, sistem ini dapat mengirimkan pemberitahuan kepada pengguna atau mengaktifkan alarm.

Perlengkapan Elektronik otomatis seperti televisi, sistem audio, atau perangkat multimedia lainnya dapat diintegrasikan dengan sistem otomatisasi rumah. Misalnya, saat memulai film di perangkat pemutar media, sistem dapat secara otomatis menurunkan pencahayaan dan menyesuaikan suara di ruangan home theater. Irigasi dan pengelolaan energi, sistem otomatisasi rumah juga dapat digunakan untuk mengontrol penggunaan air dan energi.



Gambar 10.6. Home Irrigation

(Sumber : extension.okstate.edu/fact-sheets/managing-pressure-in-the-home-irrigation-system.html)

Pengaturan irigasi otomatis dapat memantau kondisi tanah dan cuaca untuk mengatur irigasi taman atau kebun secara efisien. Selain itu, sistem manajemen energi dapat mengoptimalkan penggunaan listrik dengan mematikan perangkat yang tidak digunakan atau menyesuaikan pengaturan suhu secara otomatis.

10.5 Monitoring dan keamanan Rumah

Monitoring dan keamanan adalah aspek penting dalam konteks otomatisasi rumah dan IoT (*Internet of Things*). Menerapkan solusi monitoring dan keamanan yang cerdas dalam rumah dapat meningkatkan tingkat keamanan, memberikan ketenangan pikiran, dan memberikan pengawasan yang efektif terhadap lingkungan rumah (Taryudi, 2018).

Monitoring rumah, solusi monitoring rumah memanfaatkan berbagai sensor, kamera, dan perangkat pintar untuk memantau lingkungan rumah. Sensor gerak dapat mendeteksi kehadiran orang atau aktivitas yang mencurigakan di area tertentu dan memberikan notifikasi kepada pemilik rumah. Sensor suhu atau

kelembaban dapat memantau kondisi lingkungan dan memberikan peringatan jika terjadi perubahan yang signifikan. Selain itu, sensor pintu atau jendela dapat memberikan peringatan jika ada upaya masuk yang tidak sah. Semua data ini dapat diakses melalui perangkat seluler atau aplikasi web, memungkinkan pemilik rumah untuk mengawasi rumah mereka secara *real-time*.



Gambar 10.7. Home Security

(Sumber : psiborg.in/how-iot-is-used-for-home-security-and-why-it-is-required)

Sistem keamanan rumah, menggunakan kombinasi sensor, kamera, alarm, dan pengunci pintu pintar untuk melindungi rumah dari potensi ancaman. Sensor gerak dan sensor pintu/jendela dapat mengaktifkan alarm jika ada aktivitas yang mencurigakan atau upaya masuk yang tidak sah. Kamera keamanan memungkinkan pemantauan visual dan merekam aktivitas di dalam dan di sekitar rumah. Pengunci pintu pintar memungkinkan akses yang terkontrol dan dapat dikendalikan dari jarak jauh, sehingga pemilik rumah dapat mengunci atau membuka pintu melalui perangkat seluler atau perintah suara.

Sistem pemantauan video merupakan komponen penting dalam solusi keamanan rumah. Kamera keamanan pintar dapat dipasang di berbagai area strategis di dalam dan di sekitar rumah untuk merekam aktivitas yang terjadi. Video ini dapat diakses secara langsung atau direkam untuk tujuan pemantauan dan penyelidikan. Beberapa kamera juga dilengkapi dengan fitur deteksi gerakan dan pemberitahuan, yang memungkinkan pengguna untuk menerima notifikasi jika ada aktivitas yang mencurigakan terdeteksi.

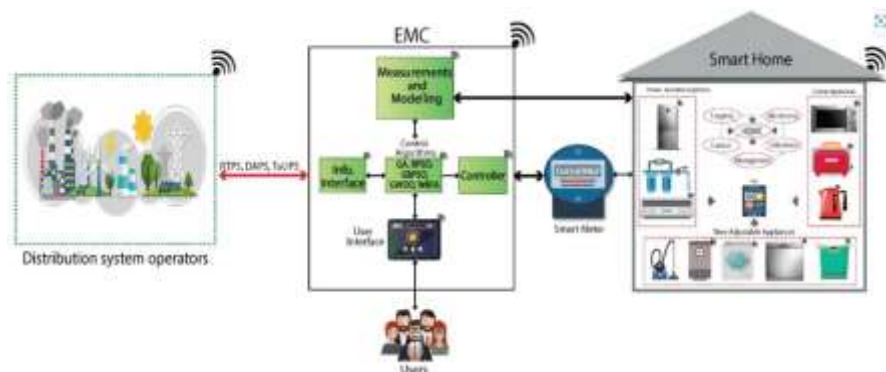
Cloud storage dan enkripsi data, Untuk menjaga keamanan data, sistem monitoring dan keamanan rumah sering menggunakan penyimpanan cloud yang aman. Ini memastikan bahwa data yang dikumpulkan oleh sensor dan kamera aman dan tersedia untuk pemilik rumah ketika diperlukan. Selain itu, enkripsi data digunakan untuk melindungi privasi dan mencegah akses yang tidak sah ke informasi sensitif.

Melalui penggunaan solusi monitoring dan keamanan yang cerdas, pemilik rumah dapat memiliki visibilitas yang lebih baik tentang lingkungan rumah mereka, melindungi rumah dari ancaman, dan merespons situasi yang tidak biasa dengan cepat serta memberikan tingkat keamanan yang lebih tinggi bagi penghuni rumah.

10.6 Manajemen Energi

Manajemen energi dalam konteks Smart Home merujuk pada penggunaan teknologi dan strategi untuk mengoptimalkan penggunaan energi di rumah dengan cara yang efisien dan berkelanjutan. Tujuan utamanya adalah untuk mengurangi konsumsi energi yang tidak perlu, menghemat biaya, dan berkontribusi pada perlindungan lingkungan. Dalam hal ini, teknologi IoT dan otomatisasi memainkan peran kunci dalam melaksanakan strategi manajemen energi yang cerdas (Hafeez, 2020).

Lebih lanjut tentang manajemen energi dalam konteks Smart Home. Monitoring Konsumsi Energi, Teknologi IoT memungkinkan pengguna untuk memantau konsumsi energi dari perangkat-perangkat rumah tangga secara real-time. Sensor energi dapat dipasang pada perangkat-perangkat ini untuk mengukur konsumsi daya dan memberikan informasi tentang seberapa banyak energi yang digunakan oleh setiap perangkat. Data ini dapat diakses melalui aplikasi atau platform khusus.



Gambar 10.8. Manajemen Energi

(Sumber : www.mdpi.com/1424-8220/20/11/3155)

Pengaturan Jadwal, dengan bantuan otomatisasi, pengguna dapat mengatur jadwal pengoperasian perangkat-perangkat tertentu. Misalnya, lampu pintar dapat diatur untuk menyala atau mati pada waktu tertentu, atau termostat pintar dapat mengatur suhu ruangan berdasarkan jadwal harian. Ini membantu menghindari penggunaan energi yang tidak perlu saat perangkat tidak digunakan.

Pengaturan Berdasarkan Kehadiran, sistem manajemen energi dapat beradaptasi dengan kehadiran penghuni rumah. Sensor kehadiran dan deteksi gerak dapat mengidentifikasi apakah ada orang di dalam ruangan. Berdasarkan informasi ini, sistem dapat mengaktifkan atau mematikan perangkat-perangkat seperti

pencahayaannya, peralatan rumah tangga, atau sistem pemanas dan pendingin ruangan.

Pengaturan Berdasarkan Kondisi Lingkungan, sistem manajemen energi dapat mengambil informasi dari sensor suhu, kelembaban, dan cahaya untuk mengatur penggunaan perangkat. Misalnya, ketika suhu eksternal rendah, sistem dapat mengoptimalkan penggunaan pemanas dan menghindari pemborosan energi.

Penggunaan Energi Terbarukan, teknologi Smart Home dapat mengintegrasikan penggunaan sumber energi terbarukan seperti panel surya. Sistem manajemen energi dapat memantau produksi energi dari panel surya dan mengatur penggunaan perangkat rumah tangga sesuai dengan ketersediaan energi yang dihasilkan.

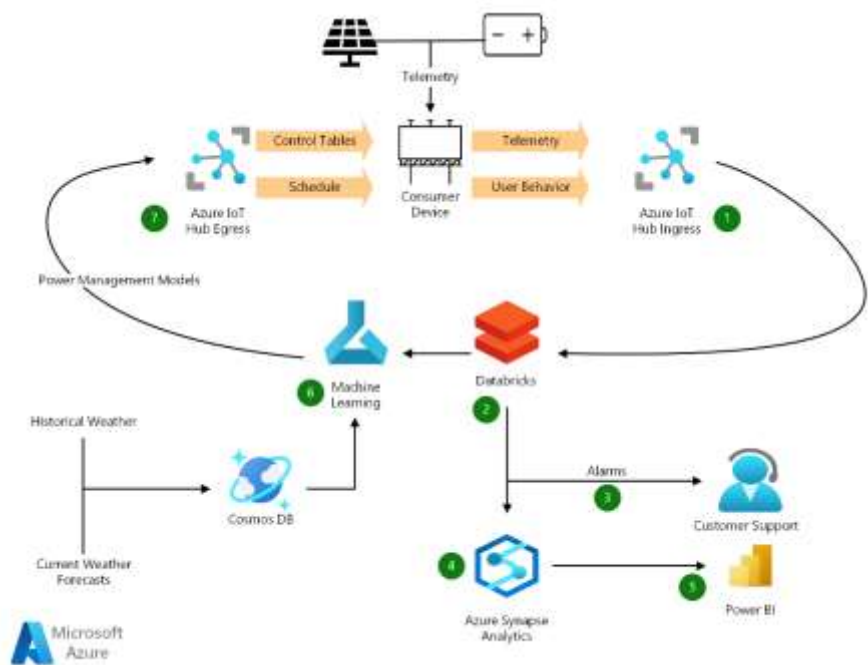
Analisis dan Rekomendasi, data energi yang dikumpulkan oleh sistem manajemen energi dapat dianalisis untuk memberikan wawasan tentang pola konsumsi energi dan potensi penghematan. Sistem ini dapat memberikan rekomendasi kepada pengguna tentang cara mengoptimalkan penggunaan energi dan mengurangi biaya.

Dengan manajemen energi yang cerdas, pengguna dapat mengurangi tagihan energi, meningkatkan efisiensi, dan berkontribusi pada perlindungan lingkungan. Teknologi IoT dan otomatisasi memungkinkan implementasi strategi yang lebih canggih dan mudah diakses, membantu menciptakan Smart Home yang lebih berkelanjutan dan efisien secara energi.

10.7 Analitik dan Pengumpulan data

Analitik dan pengumpulan data dalam konteks otomatisasi rumah merujuk pada penggunaan teknik pengumpulan, pemrosesan, dan analisis data untuk mendapatkan wawasan yang berharga tentang penggunaan, performa, dan pola perilaku perangkat rumah tangga yang terhubung (Leila, 2019).

Pengumpulan data, dalam sistem otomatisasi rumah yang terhubung dengan IoT, berbagai perangkat rumah tangga seperti lampu pintar, termostat pintar, pengunci pintu pintar, sensor suhu, dan sensor lainnya menghasilkan data yang relevan. Data ini termasuk informasi seperti status perangkat, penggunaan energi, suhu, kehadiran penghuni, dan pola interaksi dengan perangkat. Data ini dikumpulkan dan direkam oleh sistem otomatisasi rumah untuk analisis lebih lanjut.



Gambar 10.9. Analitik dan Pengumpulan data
(Sumber : learn.microsoft.com/id-id/azure/architecture/solution-ideas/articles/iot-power-management)

Pemrosesan data, setelah data terkumpul, langkah selanjutnya adalah memproses dan mengorganisir data tersebut. Pemrosesan

data mencakup pembersihan, penyaringan, penggabungan, dan pengaturan data agar siap digunakan untuk analisis. Hal ini melibatkan penggunaan algoritma dan teknik pengolahan data untuk memastikan integritas dan kualitas data yang baik.

Analisis data, setelah data diproses, analisis data dilakukan untuk mengidentifikasi pola, tren, dan wawasan yang berharga. Analisis data dalam konteks otomatisasi rumah dapat melibatkan teknik seperti analisis statistik, analisis prediktif, dan analisis pola. Contoh penggunaan analitik data dalam otomatisasi rumah termasuk mengidentifikasi pola penggunaan energi yang tidak efisien, mendeteksi anomali atau peristiwa tidak biasa, dan memberikan rekomendasi untuk mengoptimalkan pengaturan rumah tangga.

Peningkatan performa dan keamanan: Analitik data juga dapat digunakan untuk meningkatkan performa dan keamanan sistem otomatisasi rumah. Dengan menganalisis data yang terkumpul, pengguna dapat mengidentifikasi area yang dapat ditingkatkan, seperti penggunaan energi yang berlebihan, pemakaian perangkat yang tidak efisien, atau masalah keamanan potensial. Dengan wawasan ini, pengguna dapat mengambil tindakan yang diperlukan untuk meningkatkan efisiensi dan keamanan rumah mereka.

Personalisasi pengalaman pengguna: Analitik data juga dapat digunakan untuk memberikan pengalaman pengguna yang lebih personal. Dengan menganalisis pola dan preferensi pengguna yang terkumpul dari data, sistem otomatisasi rumah dapat menyesuaikan pengaturan dan perilaku perangkat sesuai dengan kebutuhan dan preferensi individu. Misalnya, sistem dapat mengatur suhu ruangan sesuai dengan preferensi penghuni atau mengatur pencahayaan sesuai dengan jadwal harian pengguna.

Melalui analitik dan pengumpulan data, pemilik rumah dapat mendapatkan wawasan yang berharga tentang penggunaan rumah tangga mereka, melakukan perbaikan dan pengoptimalan

yang diperlukan, serta meningkatkan efisiensi, kenyamanan, dan keamanan rumah mereka.

10.8 Penutup

Sebagai penutup, *Internet of Things* (IoT) telah mengubah cara mengartikan rumah. Melalui konsep Smart Home yang didukung oleh IoT, rumah bukan lagi sekadar tempat tinggal, tetapi menjadi lingkungan yang cerdas, terhubung, dan dapat diatur dengan cara yang belum pernah terjadi sebelumnya. IoT membawa inovasi yang memungkinkan perangkat-perangkat di dalam rumah untuk berkomunikasi, berinteraksi, dan bekerja bersama demi kenyamanan, efisiensi, dan keamanan rumah. Pengenalan IoT ke dalam Smart Home memberikan wawasan yang lebih dalam tentang bagaimana teknologi dapat memberdayakan kehidupan sehari-hari. Dari pengaturan perangkat hingga pengelolaan energi, IoT telah membuka pintu menuju masa depan rumah yang lebih pintar, lebih efisien, dan lebih responsif terhadap kebutuhan. Dengan terus memahami potensi dan tantangan yang ada, dan dapat menjadikan rumah sebagai pusat kehidupan modern yang terkoneksi dan lebih baik dalam setiap aspeknya.

DAFTAR PUSTAKA

- Chowdhury Arif, Doehrman Austin, Zuccollo Josh, 2017, IOT : Smart House, Indiana University Purdue University Fort Wayne
- Davies John, Fortuna Carolina, 2020, The Internet of Things, From data to Insight. Wiley
- Hafeez Ghulam, Wadud Zahid, Ullah Khan Imran, Khan Imran, Shafiq
- Zeeshan, Usman Muhammad and Ali Khan Mohammad Usman, MDPI.com, Efficient Energy Management of IoT-Enabled Smart Homes Under Price-Based Demand Response Program in Smart Grid *Sensors* 2020, 20(11), 3155; <https://doi.org/10.3390/s20113155>
- Kavitha, D., & Harshavardhan, M. 2022. Smart home automation with IoT enabled by using abode cybernation. *International Journal of Health Sciences*, 6(S2), 10342²10353. <https://doi.org/10.53730/ijhs.v6nS2.7650>
- Leila Damghani, Hamidreza Damghani, Heliasadat Hosseinian, Hossein Mohammadnezhad Shourkaei, 2019, Data Analysis, Analytics in Internet of Things and BigData, *4th International conference on Combinatorics, Cryptography, Computer Science and computing*, Nov 2019, Iran University of Science and Technology
- Mada Albany, Enas Alsahafi, Itidal Alruwili, Salim Elkhediri, 2022 A review: Secure Internet of thing System for Smart Houses *The 13th International Conference on Ambient Systems, Networks and Technologies (ANT)*, 2022, Porto, Portugal, ScienceDirect

- Taryudi, Davin Bagas Adriano and Wahyu Apsari Ciptoning Budi, 2018, Iot-based Integrated Home Security and Monitoring System, OP Conf. Series: Journal of Physics: Conf. Series 1140 (2018) IOP Publishing, doi:10.1088/1742-6596/1140/1/012006
- Yaddarabullah, Deden Ardiansyah, 2017, Mengarungi Internet of Things bagi pemula, Universitas Trilogi, Jakarta
- Zubair Sharif, Low Tang Jung, Muhammad Ayaz, Mazlaini Yahya, Dodo Khan, 2022, Smart Home Automation by Internet-of-Things Edge Computing Platform, Vol. 13, No. 4, 2022 (IJACSA) International Journal of Advanced Computer Science and Applications Websites (diakses pada Agustus 2023)
- Anderson Robert, techparasol, Is A Smart TV An IOT Device? (Explained For Beginners) <https://techparasol.com/smart-tv-iot-device/>
- Beebom Staff, LG Reveals New ThinQ Smart Speaker Powered by Google Assistant <https://beebom.com/lg-thinq-smart-speaker/>
- Cert.govt.nz, Smart devices - The Internet of Things (IoT) <https://www.cert.govt.nz/individuals/guides/smart-devices-the-internet-of-things-iot/>
- Kevin Moore, Justin Quetone Moss, Managing Pressure in the Home Irrigation System <https://extension.okstate.edu/fact-sheets/managing-pressure-in-the-home-irrigation-system.html>
- Learn.microsoft.com, Lampu, daya, dan internet yang terhubung dengan IoT <https://learn.microsoft.com/id-id/azure/architecture/solution-ideas/articles/iot-power-management>
- Rayming PCB & Assembly, What is the Significance of Smartwatch IoT. <https://www.raypcb.com/smartwatch-iot/>
- Sorice Cory, IoTWorldToday, The Value Chain Is Evolving for Connected-Home Companies

<https://www.iotworldtoday.com/smart-cities/the-value-chain-is-evolving-for-connected-home-companies>

Trakaid, How IoT Devices are making home automation and connected living a reality in 2020

<https://www.trakaid.com/how-iot-devices-are-making-home-automation-and-connected-living-a-reality-in-2020/>

Vidushi, How IoT is used for Home Security and why it is required?

<https://psiborg.in/how-iot-is-used-for-home-security-and-why-it-is-required/>

BAB 11

ANALITIK DATA DAN KECERDASAN BUATAN DALAM INTERNET OF THINGS

Oleh Niko Akbar

11.1 Analitik Data

Kegiatan mengorganisasikan data, menjabarkan kedalam unit-unit, melakukan sintesa, menyusun kedalam pola, memilih mana yang penting dan yang akan dipelajari, dan membuat kesimpulan (Tahar, Setiadi and Rahayu, 2022). Sebuah kesimpulan akan menjadi sebuah keputusan seorang pemangku kebijakan dan beberapa orang didalam organisasi agar dapat mampu menadapatkan hasil untuk organisasinya. Beberapa analitik data dikerjakan oleh seorang analis yang terampil dalam mengolah dan memanipulasi data. Dengan menggunakan komputer dan tekniknya sehingga output yang dihasilkan dapat berupa sebuah data yang akurat dan berharga.

11.2 Kecerdasan Buatan (*Artificial Intelligence* /AI)

Merupakan kecerdasan yang ditambahkan pada suatu sistem atau dengan kata lain kemampuan sistem untuk menafsirkan data eksternal dengan benar serta mengelola data dan menggunakan hasil olahan untuk suatu tujuan tertentu (de Sousa *et al.*, 2019; Goralski and Tan, 2020). Setiap penemuan dalam bidang elektronik, teknik, dan beberapa ilmu lainnya telah dipengaruhi oleh AI, AI bukan hanya tentang robot, tetapi AI juga memahami

sifat pemikiran dan tindakan cerdas menggunakan komputer sebagai perangkat – perangkat eksperimental. Beberapa penelitian mengemukakan bahwa eropa dan AS merupakan negara pionier dalam pengaplikasian AI(de Sousa *et al.*, 2019; Shank and Gott, 2019). Penelitian terdahulu menyatakan bahwa AI adalah sistem yang disusun untuk berinteraksi kepada semua orang di dunia dengan kemampuan khusus dan kebiasaan *Intelligence* seperti manusia (de Sousa *et al.*, 2019; Shank and Gott, 2019; Goralski and Tan, 2020)

11.3 Hubungan analitik data dan Kecerdasan Buatan pada IOT

Zaman serba digital (*Digital Technology*) saat ini mendatangkan sebuah kehidupan yang serba instan, segala sesuatu serba cepat, serta informasi tersebar dalam hitungan detik. Hal tersebut mencerminkan bahwa dunia telah memasuki revolusi industri 4.0 yang merupakan adanya perubahan bagi setiap manusia dalam segala bidang(Putrawangsa and Hasanah, 2018). Dalam revolusi industri 4.0, Teknologi digital dan kemampuan fisik digabungkan dengan kecerdasan buatan dan data-data pendukung merupakan hasil integrasi dengan *Internet of Things* menghasilkan *output* digital yang memudahkan kehidupan manusia (Hamdan, 2018).

Berdasarkan data yang diperoleh dari McKinsey, penggunaan internet semakin meningkat hingga 25%(Dahlqvist *et al.*, 2019). Bahkan riset dari APJII mengatakan persentase penetrasi Internet di indonesia sebesar 3,32% dari tahun 2020 – 2023 sebesar 73,70% menjadi 77,02%. Internet berevolusi dan mentransformasikan dari penyimpanan dokumen statis ke dunia maya dengan berbagai pengguna, perangkat, dan aplikasi yang saling terhubung. Evolusi internet terjadi karena peran dari *internet of things* (IoT) yang memiliki sasaran utama dalam penggunaan dan pengolahan data yang perpaduan dengan

informasi yang dihasilkan dalam kehidupan sehari-hari (Kiryakova, Yordanova and Angelova, 2017).

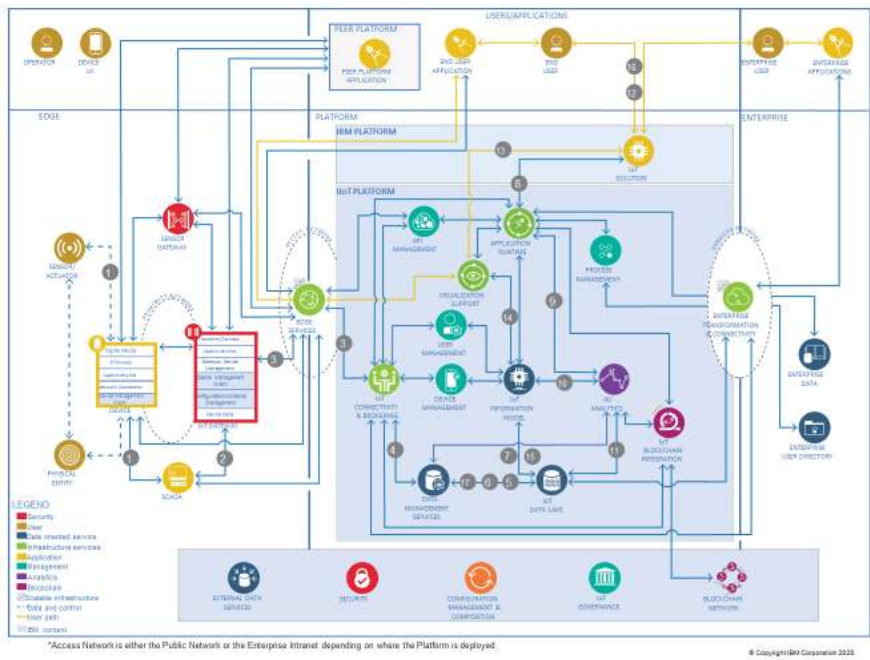
IoT adalah sebuah jaringan perangkat yang tersambung dan berguna untuk mendukung proses komunikasi antar perangkat terdapat beberapa teknologi yang menggunakan IoT seperti : sensor, aktuator, sistem operasi, Microcontroller, teknologi komunikasi, sekuritas, platform IoT, dan alat analitis(Genadiarto, Noertjahyana and Kabzar, 2017). IoT memiliki beberapa komponen penting, dapat menjalankan berbagai perintah dengan cara(Megawati, 2021):

1. Perangkat akan terhubung dengan platform IoT,
2. Perangkat yang mengintegrasikan data-data dari berbagai perangkat dengan bantuan internet.
3. Penerapan cara analisis terhadap data yang diperoleh.
4. Platform IoT yang kuat dapat menunjukkan dengan tepat Informasi apa yang berguna dan apa yang dapat diabaikan dengan aman.
5. Informasi dapat digunakan untuk mendeteksi pola, membuat rekomendasi, dan mendeteksi kemungkinan masalah sebelum terjadi.

Beberapa teknologi AI juga banyak digunakan untuk banyak tujuan, misal diantaranya deteksi dini dan memprediksi wabah, pembuatan robot, memproduksi CT-Scan yang berguna untuk mendeteksi Pneumonia(Mubaroq and Insyiroh, 2020), mengidentifikasi foto rontgen paru-paru yang terkena COVID-19 (Mei *et al.*, 2020; Ting *et al.*, 2020)

Selain itu, IoT juga diterapkan dalam Industri Perusahaan Teknologi seperti IBM. Dalam IoT pada sebuah Industri Perusahaan terdapat Referensi Arsitektur yang berdasarkan pendekatan dari perusahaan IBM untuk solusi IoT. Solusinya berupa penggunaan Informasi dari perangkat, orang-orang, dan aplikasi dengan cloud atau layanan server Internal perusahaan

serta sebuah sistem untuk menghasilkan Pemahaman dan sebuah nilai.



Gambar 11.2. Arsitektur IoT IBM(Libow, no date)

Gambar Diatas merupakan sebuah Referensi Arsitektur diatas merupakan titik awal proyek pelanggan dan solusi yang ditawarkan berupa platform IoT.(Libow, no date).

Selain itu, beberapa IoT punya beberapa dampak signifikan dalam beberapa aspek dalam kehidupan kita, dalam bidang industri, dan sekelompok masyarakat. Contohnya :

1. Peningkatan Efisiensi & Produktivitas.
2. Pengalaman Pelanggan yang Lebih Baik.
3. Wawasan & Pengambilan Keputusan Berbasis Data.
4. Optimalisasi Rantai Pasokan.

Dalam penjelasan lengkapnya.

1. Peningkatan Efisiensi dan Produktivitas
 - a. Otomasi Industri: Sistem IoT yang meningkatkan produktivitas dengan mengotomatisasi proses industri, misalnya: Manufaktur.
 - b. Optimalisasi rantai pasokan: IoT meningkatkan manajemen rantai pasokan dengan memberikan visibilitas waktu nyata. Misalnya: melacak pengiriman
2. Peningkatan Pengalaman Pelanggan :
 - a. Ritel yang sudah dipersonalisasi. IoT membuat pembeli dapat merasakan pengalaman mencari produk yang sesuai dengan diinginkan berdasarkan perilaku dan data personal pelanggan.
 - b. Mobil yang terhubung dengan IoT : Integrasi IoT pada mobil membuat pelanggan merasakan pengalaman berkendara lebih baik.
3. Wawasan berbasis data (*Data-Driven Insights*) & Pengambilan Keputusan (*Decision Makings*)
 - a. Pemeliharaan prediktif : IoT memungkinkan pemeliharaan yang dapat diprediksi berdasarkan data yang sudah dikumpul dan dianalisis dalam waktu yang nyata berdasarkan sensor yang tertanam dalam peralatan.
 - b. Perencanaan *Smart City* : Data yang dihasilkan IoT memberikan wawasan untuk perencanaan kota dan alokasi sumber daya.

Jadi Disimpulkan bahwa *Internet of Things* tidak lepas dari Kolaborasi hasil teknologi, berupa Analitik Data (Data Analytics) dan Kecerdasan Buatan (AI)

DAFTAR PUSTAKA

- Dahlqvist, F. *et al.* 2019. 'Growing opportunities in the Internet of Things', *McKinsey & Company*, pp. 1–6.
- Genadiarto, A. S., Noertjahyana, A. and Kabzar, V. 2017. 'Introduction of Internet of Thing technology based on prototype', *Jurnal Informatika*, 14(1), pp. 47–52.
- Goralski, M. A. and Tan, T. K. 2020. 'Artificial intelligence and sustainable development', *The International Journal of Management Education*, 18(1), p. 100330.
- Hamdan, H. 2018. 'Industri 4.0: Pengaruh revolusi industri pada kewirausahaan demi kemandirian ekonomi', *Jurnal Nusantara Aplikasi Manajemen Bisnis*, 3(2), pp. 1–8.
- Kiryakova, G., Yordanova, L. and Angelova, N. (2017) 'Can we make Schools and Universities smarter with the Internet of Things?', *TEM Journal*, 6(1), p. 80.
- Libow, E. (IBM) (no date) *Internet of Things architecture*. Available at: <https://www.ibm.com/cloud/architecture/architectures/iotArchitecture/reference-architecture/> (Accessed: 3 July 2023).
- Megawati, S. 2021. 'Pengembangan Sistem Teknologi Internet of Things Yang Perlu Dikembangkan Negara Indonesia', *Journal of Information Engineering and Educational Technology*, 5(1), pp. 19–26. doi: 10.26740/jieet.v5n1.p19-26.
- Mei, X. *et al.* 2020. 'Artificial intelligence-enabled rapid diagnosis of patients with COVID-19', *Nature Medicine*, 26(8), pp. 1224–1228. doi: 10.1038/s41591-020-0931-3.
- Mubaroq, S. and Insiyroh, I. M. 2020. 'Teknologi Kecerdasan Buatan, Big Data Analysis, Dan Internet of Things: Potensi Dan Perannya Dalam Penanganan Covid-19 Di Indonesia', *Jurnal Kependudukan Indonesia*, 2902, p. 109. doi: 10.14203/jki.v0i0.580.

- Putrawangsa, S. and Hasanah, U. 2018. 'Integrasi teknologi digital dalam pembelajaran di era industri 4.0: Kajian dari perspektif pembelajaran matematika', *Jurnal Tatsqif*, 16(1), pp. 42–54.
- Shank, D. B. and Gott, A. 2019. 'People's self-reported encounters of Perceiving Mind in Artificial Intelligence', *Data in brief*, 25, p. 104220.
- de Sousa, W. G. *et al.* 2019. 'How and where is artificial intelligence in the public sector going? A literature review and research agenda', *Government Information Quarterly*, 36(4), p. 101392.
- Tahar, A., Setiadi, P. B. and Rahayu, S. 2022. 'Strategi Pengembangan Sumber Daya Manusia dalam Menghadapi Era Revolusi Industri 4.0 Menuju Era Society 5.0', *Jurnal Pendidikan Tambusai*, 6(2), pp. 12380–12394. Available at: <https://jptam.org/index.php/jptam/article/view/4428>.
- Ting, D. S. W. *et al.* 2020. 'Digital technology and COVID-19', *Nature medicine*, 26(4), pp. 459–461.

BAB 12

TANTANGAN DAN PELUANG MASA DEPAN DALAM INTERNET OF THINGS

Oleh Iwan Adhicandra

12.1 Pendahuluan

12.1.1 Pengenalan tentang *Internet of Things* (IoT):

Internet of Things (IoT) adalah konsep di mana objek fisik, perangkat, atau benda lainnya dapat saling terhubung dan berkomunikasi melalui jaringan internet. Dalam IoT, perangkat-perangkat ini dapat dikendalikan, dipantau, dan bertukar data secara otomatis tanpa adanya interaksi manusia secara langsung. IoT mencakup berbagai perangkat seperti sensor, kendaraan pintar, perangkat rumah tangga pintar, peralatan industri, dan banyak lagi. Koneksi dan kolaborasi antara perangkat ini memberikan potensi besar untuk meningkatkan efisiensi, produktivitas, dan kenyamanan dalam berbagai aspek kehidupan.

12.1.2 Latar Belakang Tantangan dan Peluang Masa Depan dalam IoT:

Pengembangan teknologi IoT telah mencapai kemajuan yang pesat, tetapi juga dihadapkan pada sejumlah tantangan yang perlu dipecahkan agar dapat mengoptimalkan manfaatnya. Beberapa tantangan utama dalam IoT termasuk masalah keamanan dan privasi data, standar dan kompatibilitas yang belum sepenuhnya seragam, keterbatasan daya dan sumber daya pada perangkat, serta kesulitan dalam mengelola infrastruktur IoT yang berkembang pesat. Selain tantangan, IoT juga menawarkan

berbagai peluang yang menarik, seperti penyempurnaan efisiensi operasional, pengembangan produk dan layanan inovatif, pemanfaatan analitik data dan kecerdasan buatan untuk pengambilan keputusan lebih baik, serta peningkatan pengalaman pengguna dalam berinteraksi dengan lingkungan sekitarnya.

12.1.3 Tujuan dan Ruang Lingkup Topik:

Tujuan dari topik ini adalah untuk menyelidiki dan membahas tantangan dan peluang masa depan dalam pengembangan dan penerapan teknologi *Internet of Things*. Poin-poin yang akan dijelaskan mencakup latar belakang konsep IoT, tantangan-tantangan yang dihadapi dalam mengimplementasikan teknologi ini, serta berbagai peluang yang dapat dimanfaatkan untuk kemajuan teknologi dan masyarakat. Ruang lingkup topik akan meliputi aspek-aspek seperti keamanan dan privasi, standar dan kompatibilitas, keterbatasan daya dan sumber daya, skalabilitas dan keterhubungan perangkat, serta dampak regulasi dan hukum dalam konteks IoT. Selain itu, topik ini juga akan mengulas studi kasus yang mencerminkan tantangan dan peluang dalam implementasi IoT di berbagai sektor dan lingkungan perkotaan. Dengan demikian, diharapkan topik ini akan memberikan pemahaman yang komprehensif tentang tantangan dan peluang yang dihadapi dalam perkembangan masa depan teknologi Internet of Things.

12.2 Tantangan dalam Internet of Things

12.2.1 Keamanan dan Privasi:

Ancaman Keamanan dalam IoT:

Salah satu tantangan utama dalam Internet of Things adalah keamanan. Dengan banyaknya perangkat yang terhubung, terbuka peluang untuk serangan siber dan ancaman keamanan lainnya. Perangkat IoT yang tidak memiliki sistem keamanan yang memadai dapat menjadi target empuk bagi peretas untuk meretas

perangkat, mencuri data sensitif, atau bahkan mengambil alih kontrol perangkat tersebut untuk tujuan yang jahat.

Kerentanan pada Perangkat IoT:

Banyak perangkat IoT didesain dengan biaya rendah dan sumber daya terbatas, yang mengakibatkan rendahnya tingkat keamanan. Hal ini menyebabkan beberapa perangkat IoT memiliki kerentanan yang mudah dieksploitasi oleh peretas. Tantangan ini mengharuskan produsen dan pengembang untuk lebih berfokus pada pengujian keamanan dan pembaruan perangkat lunak secara teratur untuk mengatasi kerentanan tersebut.

Proteksi Data Pengguna dan Privasi:

IoT mengumpulkan data dari berbagai perangkat yang terhubung, termasuk data pribadi pengguna. Tantangan utama adalah memastikan data tersebut dijaga dengan baik dan tidak disalahgunakan. Perlindungan data pengguna dan privasi menjadi prioritas penting untuk menghindari penyalahgunaan data dan potensi pelanggaran privasi yang dapat merugikan pengguna.

12.2.2 Standar dan Kompatibilitas:

Keterbatasan Standar Industri:

Saat ini, industri IoT masih menghadapi tantangan dalam mengadopsi standar yang seragam dan konsisten. Keterbatasan standar dapat menghambat interoperabilitas antara berbagai perangkat IoT yang diproduksi oleh berbagai vendor. Tanpa standar yang jelas, integrasi dan kompatibilitas antar perangkat IoT menjadi lebih sulit.

Kompatibilitas Perangkat IoT:

Perangkat IoT yang berasal dari produsen yang berbeda seringkali menggunakan protokol dan teknologi yang berbeda pula. Ini bisa menyulitkan integrasi dan interaksi antar perangkat IoT. Dalam beberapa kasus, perangkat IoT mungkin tidak dapat

berfungsi secara optimal atau bahkan tidak dapat berkomunikasi sama sekali jika tidak kompatibel satu sama lain.

12.2.3 Keterbatasan Daya dan Sumber Daya:

Masalah Daya pada Perangkat IoT:

Beberapa perangkat IoT beroperasi pada daya baterai atau sumber daya terbatas lainnya. Penggunaan daya yang efisien menjadi penting karena perangkat IoT yang terhubung dan selalu aktif dapat menguras daya baterai dengan cepat. Tantangan ini mendorong para pengembang untuk mencari cara-cara inovatif untuk mengoptimalkan penggunaan daya dan memperpanjang masa pakai baterai.

Pengelolaan Sumber Daya yang Terbatas:

Selain masalah daya, sebagian besar perangkat IoT juga memiliki sumber daya terbatas seperti kapasitas penyimpanan dan prosesor yang relatif rendah. Tantangan ini mendorong pengembang untuk mengoptimalkan penggunaan sumber daya dan menyusun strategi efisien untuk mengelola dan memproses data yang dikumpulkan dari perangkat IoT.

12.2.4 Skalabilitas dan Keterhubungan:

Tantangan dalam Skalabilitas Infrastruktur IoT:

Seiring dengan pertumbuhan jumlah perangkat IoT yang terhubung, infrastruktur yang ada harus dapat mengakomodasi skala yang lebih besar. Tantangan ini mencakup kapasitas jaringan yang cukup, manajemen data yang efisien, dan kemampuan infrastruktur untuk menangani jumlah perangkat yang semakin bertambah.

Integrasi dan Interoperabilitas Perangkat IoT:

Integrasi dan interoperabilitas antara berbagai perangkat IoT yang berbeda merupakan tantangan lain. Penting bagi perangkat IoT untuk dapat berkomunikasi dan berinteraksi dengan

perangkat lainnya untuk memberikan solusi yang holistik dan efisien bagi pengguna.

12.2.5 Regulasi dan Hukum:

Isu Regulasi tentang IoT:

Perkembangan cepat teknologi IoT telah melampaui regulasi dan undang-undang yang ada. Tantangan ini mendorong pihak berwenang untuk mencari cara untuk mengatur penggunaan teknologi IoT secara efektif. Hal ini termasuk kebijakan keamanan data, perlindungan privasi, dan tanggung jawab hukum terkait penggunaan perangkat IoT.

Tantangan Hukum dalam Penggunaan IoT:

Penggunaan teknologi IoT sering kali menimbulkan masalah hukum baru. Salah satu contohnya adalah pertanyaan tentang siapa yang bertanggung jawab jika terjadi kegagalan perangkat IoT atau kerugian akibat data yang salah. Tantangan hukum ini memerlukan kerjasama antara regulator, produsen perangkat IoT, dan pemilik perangkat untuk menciptakan lingkungan yang adil dan aman untuk semua pihak terlibat.

12.3 Peluang dalam Internet of Things

12.3.1 Penyempurnaan Efisiensi Operasional:

IoT dalam Peningkatan Proses Bisnis:

Dengan mengintegrasikan teknologi IoT dalam proses bisnis, perusahaan dapat meningkatkan efisiensi operasional secara signifikan. Perangkat IoT dapat mengumpulkan data secara real-time tentang produksi, inventaris, dan rantai pasokan, memungkinkan pemantauan dan pengelolaan yang lebih baik. Data ini dapat digunakan untuk meningkatkan kinerja operasional, mengidentifikasi potensi penyempitan, mengurangi waktu henti, dan mengoptimalkan biaya produksi.

Otomatisasi dan Optimalisasi Kinerja:

IoT memungkinkan otomatisasi proses bisnis yang sebelumnya memerlukan intervensi manual. Perangkat IoT dapat berkomunikasi secara otomatis dan mengambil tindakan berdasarkan data yang dikumpulkan. Misalnya, perangkat IoT di lingkungan manufaktur dapat mengontrol mesin secara otomatis, mengatur suhu dan cahaya, dan mengoptimalkan konsumsi energi untuk meningkatkan kinerja operasional secara keseluruhan.

12.3.2 Pengembangan Produk dan Layanan Baru:

Inovasi Produk Berbasis IoT:

IoT membuka peluang besar bagi inovasi produk. Perusahaan dapat menciptakan produk baru yang terhubung ke internet dan menawarkan fitur-fitur pintar yang sebelumnya tidak mungkin. Contohnya, mobil pintar dengan koneksi internet yang dapat mengakses informasi lalu lintas secara real-time atau perangkat rumah tangga pintar yang dapat dioperasikan dari jarak jauh melalui aplikasi smartphone.

Layanan Baru Berdasarkan IoT:

Penggunaan teknologi IoT memungkinkan perusahaan untuk menawarkan layanan baru yang berbasis pada data dan konektivitas. Misalnya, perusahaan asuransi dapat menggunakan data dari perangkat IoT untuk menawarkan polis asuransi yang dipersonalisasi berdasarkan perilaku pengguna. Layanan berbasis IoT juga dapat mencakup pemantauan kesehatan jarak jauh, manajemen energi rumah, atau analitik prediktif untuk meningkatkan pengalaman pelanggan.

12.3.3 Analitik Data dan Kecerdasan Buatan (AI):

Pemanfaatan Data IoT untuk Pengambilan Keputusan:

Data yang dikumpulkan dari perangkat IoT dapat memberikan wawasan berharga bagi perusahaan untuk membuat keputusan yang lebih cerdas. Dengan menggunakan analitik data,

perusahaan dapat menganalisis tren, pola, dan hubungan yang tersembunyi dalam data IoT untuk merumuskan strategi bisnis yang lebih baik dan efektif.

Implementasi Kecerdasan Buatan dalam IoT:

Kecerdasan buatan (AI) dapat diterapkan pada data yang dikumpulkan dari perangkat IoT untuk meningkatkan fungsionalitas dan kinerja perangkat. AI dapat membantu perangkat IoT belajar dari pola dan perilaku pengguna, memprediksi kejadian tertentu, dan merespons secara otomatis tanpa intervensi manusia. Dengan demikian, implementasi AI dalam IoT meningkatkan kemampuan adaptasi dan kinerja perangkat secara keseluruhan.

12.3.4 Peningkatan Pengalaman Pengguna: Personalisasi dan Kemudahan Penggunaan:

IoT memungkinkan personalisasi yang lebih besar dalam produk dan layanan. Perangkat IoT dapat mengumpulkan data tentang preferensi dan kebiasaan pengguna, yang dapat digunakan untuk menyesuaikan pengalaman pengguna. Contohnya, aplikasi berbasis IoT dapat mengatur preferensi pengguna untuk suhu dan pencahayaan di rumah, sehingga memberikan kenyamanan maksimal.

IoT dalam Meningkatkan Interaksi Pengguna dengan Lingkungan:

Dengan banyaknya perangkat IoT yang terhubung, pengguna dapat berinteraksi lebih baik dengan lingkungan sekitarnya. Misalnya, dengan menggunakan asisten virtual berbasis IoT, pengguna dapat mengontrol perangkat rumah tangga, mengatur jadwal, atau mencari informasi hanya dengan menggunakan suara. Hal ini meningkatkan efisiensi dan kenyamanan pengguna dalam berinteraksi dengan teknologi di sekitarnya.

12.4 Perbandingan Tantangan dan Peluang dalam IoT

12.4.1 Analisis Perbandingan Tantangan dan Peluang:

Dalam menghadapi perkembangan Internet of Things (IoT), terdapat tantangan dan peluang yang perlu diperhatikan secara serius. Berikut adalah analisis perbandingan antara tantangan dan peluang dalam IoT:

Keamanan dan Privasi:

Tantangan: Ancaman keamanan siber pada perangkat IoT dan kerentanan dapat menyebabkan potensi risiko bagi pengguna dan infrastruktur. Selain itu, perlindungan data pengguna dan privasi menjadi isu krusial dalam penggunaan teknologi ini.

Peluang: Meningkatkan keamanan perangkat IoT dengan penggunaan enkripsi, otorisasi akses, dan pembaruan perangkat lunak teratur. Pemanfaatan teknologi kecerdasan buatan untuk mendeteksi ancaman dan perlindungan data dapat meningkatkan keamanan dan privasi dalam IoT.

Standar dan Kompatibilitas:

Tantangan: Kurangnya standar yang seragam mengakibatkan kesulitan dalam integrasi dan kompatibilitas antar perangkat IoT dari berbagai vendor.

Peluang: Mendorong industri untuk mencapai kesepakatan tentang standar dan protokol yang seragam. Inisiatif standarisasi dapat membantu meningkatkan interoperabilitas dan kesesuaian antar perangkat IoT.

Keterbatasan Daya dan Sumber Daya:

Tantangan: Perangkat IoT seringkali beroperasi dengan daya baterai atau sumber daya terbatas lainnya, yang dapat mempengaruhi kinerja dan masa pakai perangkat.

Peluang: Penggunaan teknologi hemat energi, perangkat yang dapat diisi ulang, dan pengelolaan sumber daya yang cerdas

dapat membantu mengatasi keterbatasan daya dan memaksimalkan efisiensi energi perangkat IoT.

Skalabilitas dan Keterhubungan:

Tantangan: Pertumbuhan pesat jumlah perangkat IoT memerlukan infrastruktur yang dapat menangani skala yang lebih besar.

Peluang: Mengembangkan infrastruktur yang skalabel dan fleksibel untuk mengakomodasi pertumbuhan IoT. Memanfaatkan teknologi jaringan baru seperti 5G dan edge computing untuk meningkatkan keterhubungan dan responsivitas perangkat IoT.

Regulasi dan Hukum:

Tantangan: Regulasi dan hukum yang belum matang dapat menyulitkan pengembangan dan adopsi teknologi IoT.

Peluang: Berpartisipasi dalam pembentukan regulasi dan kebijakan yang berkaitan dengan IoT untuk menciptakan lingkungan yang aman dan mendukung pertumbuhan teknologi. Transparansi dan kepatuhan terhadap peraturan dapat meningkatkan kepercayaan masyarakat terhadap IoT.

12.4.2 Strategi Mengatasi Tantangan dan Memanfaatkan Peluang:

Investasi dalam Keamanan dan Privasi:

Mengintegrasikan solusi keamanan yang kuat, termasuk enkripsi, otentikasi, dan perangkat lunak keamanan, dalam desain dan pengembangan perangkat IoT.

Memperbarui perangkat lunak secara teratur untuk mengatasi kerentanan dan memastikan perlindungan data pengguna dan privasi.

Mendorong Standarisasi dan Interoperabilitas:

Berpartisipasi dalam komunitas standarisasi dan mendukung pengembangan protokol dan standar yang seragam untuk memastikan kompatibilitas antar perangkat IoT.

Menggunakan platform dan framework yang berbasis standar untuk memfasilitasi integrasi dan keterhubungan yang lebih mudah.

Pengembangan Perangkat IoT Hemat Energi:

Mengoptimalkan penggunaan daya dan sumber daya pada perangkat IoT dengan desain yang hemat energi dan teknologi efisien.

Menggunakan teknologi terbaru seperti LPWAN (*Low-Power Wide Area Network*) untuk mengurangi konsumsi daya perangkat IoT.

Skalabilitas Infrastruktur dan Keterhubungan:

Mengadopsi teknologi jaringan seperti 5G dan edge computing untuk memastikan infrastruktur yang dapat menangani pertumbuhan IoT yang pesat.

Memperluas cakupan jaringan dan menjamin konektivitas yang stabil dan handal untuk perangkat IoT.

Mendukung Peraturan dan Kepatuhan:

Melibatkan pemangku kepentingan, regulator, dan organisasi terkait untuk mengembangkan regulasi yang relevan dan memastikan IoT beroperasi sesuai dengan standar keamanan dan privasi yang ditetapkan.

Transparansi dalam pengumpulan dan penggunaan data untuk mendapatkan kepercayaan pengguna dan menghindari masalah hukum yang potensial.

Dengan mengatasi tantangan dan memanfaatkan peluang yang dihadapi dalam Internet of Things, teknologi ini memiliki potensi besar untuk memberikan dampak positif dalam berbagai

bidang kehidupan, meningkatkan efisiensi, inovasi, dan kenyamanan bagi pengguna serta membuka peluang baru untuk bisnis dan industri.

12.5 Studi Kasus

12.5.1 Kasus Tantangan dalam Implementasi IoT pada Sektor Industri:

Studi Kasus: Penerapan IoT dalam Pabrik Manufaktur Tantangan:

Sebuah pabrik manufaktur berencana untuk mengadopsi teknologi *Internet of Things* (IoT) untuk meningkatkan efisiensi operasional. Namun, mereka menghadapi beberapa tantangan dalam implementasi IoT:

Keamanan dan Privasi: Pabrik harus memastikan bahwa sistem IoT yang diterapkan aman dari serangan siber, sehingga tidak ada peretas yang dapat mengganggu proses produksi atau mencuri data sensitif tentang bisnis mereka.

Keterbatasan Daya dan Sumber Daya: Banyak perangkat IoT yang terhubung di pabrik ini beroperasi dengan daya baterai. Oleh karena itu, penting untuk mengoptimalkan penggunaan daya dan memperpanjang masa pakai baterai perangkat IoT.

Keterhubungan dan Skalabilitas: Pabrik memiliki ratusan perangkat dan mesin yang berbeda, dan beberapa di antaranya mungkin diproduksi oleh vendor yang berbeda. Integrasi dan keterhubungan antara perangkat IoT ini harus dipertimbangkan agar sistem bekerja dengan baik secara keseluruhan.

12.5.2 Kasus Peluang dalam Penggunaan IoT pada Lingkungan Perkotaan:

Studi Kasus: Kota Cerdas (*Smart City*) Peluang:

Sebuah kota ingin mengimplementasikan konsep *Smart City* dengan menggunakan teknologi *Internet of Things* (IoT) untuk

meningkatkan kualitas hidup penduduk dan efisiensi dalam pengelolaan kota. Beberapa peluang yang dihadapi dalam penggunaan IoT pada lingkungan perkotaan:

Peningkatan Manajemen Lalu Lintas: Dengan menggunakan sensor IoT yang terpasang pada jalan dan persimpangan, kota dapat mengumpulkan data lalu lintas secara real-time. Data ini dapat digunakan untuk mengoptimalkan sinkronisasi lampu lalu lintas, mengurangi kemacetan, dan meningkatkan keamanan jalan.

Pengelolaan Limbah yang Efisien: Sensor IoT yang terpasang di tempat pembuangan sampah dapat memberikan informasi tentang tingkat penuhnya wadah sampah. Data ini dapat membantu mengoptimalkan rute pengumpulan sampah dan mengurangi biaya pengelolaan limbah.

Monitoring Kualitas Udara: Sensor IoT dapat digunakan untuk mengukur kualitas udara di berbagai lokasi di kota. Data ini dapat digunakan untuk mengidentifikasi polusi udara dan mengambil tindakan pencegahan yang tepat untuk meningkatkan kualitas udara perkotaan.

Pelayanan Publik yang Lebih Baik: Melalui aplikasi berbasis IoT, warga kota dapat dengan mudah melaporkan masalah infrastruktur seperti kerusakan jalan, lampu jalanan yang rusak, atau kebocoran air. Hal ini memungkinkan respon yang lebih cepat dari pihak berwenang untuk memperbaiki masalah tersebut.

Dengan mengambil peluang dari teknologi IoT, kota cerdas dapat mencapai efisiensi yang lebih tinggi dalam pengelolaan sumber daya, memberikan layanan publik yang lebih baik, dan meningkatkan kualitas hidup bagi penduduknya. Selain itu, implementasi IoT dalam lingkungan perkotaan juga dapat berkontribusi pada pengurangan dampak lingkungan dan keberlanjutan kota di masa depan.

12.6 Kesimpulan

12.6.1 Ringkasan Tantangan dan Peluang Masa Depan dalam IoT:

Internet of Things (IoT) menawarkan potensi besar untuk mengubah cara kita berinteraksi dengan perangkat dan lingkungan di sekitar kita. Namun, dengan potensi tersebut juga datang sejumlah tantangan yang perlu diatasi agar IoT dapat diimplementasikan dengan aman dan efektif. Beberapa tantangan utama dalam IoT mencakup:

Keamanan dan Privasi: Ancaman keamanan siber dan risiko kerentanan pada perangkat IoT dapat menyebabkan kerugian serius bagi pengguna dan bisnis.

Standar dan Kompatibilitas: Keterbatasan standar dan kompatibilitas antar perangkat IoT dapat menghambat integrasi dan interaksi yang optimal.

Keterbatasan Daya dan Sumber Daya: Perangkat IoT yang beroperasi dengan daya baterai atau sumber daya terbatas memerlukan manajemen yang efisien dan hemat energi.

Skalabilitas dan Keterhubungan: Pertumbuhan pesat jumlah perangkat IoT menuntut infrastruktur yang dapat mengakomodasi skala yang lebih besar dan keterhubungan yang lancar.

Regulasi dan Hukum: Kurangnya regulasi yang matang dan kepatuhan terhadap hukum dapat menyulitkan perkembangan dan adopsi teknologi IoT.

Namun, seiring dengan tantangan, IoT juga menawarkan berbagai peluang yang menarik, termasuk:

Penyempurnaan Efisiensi Operasional: IoT dapat meningkatkan efisiensi proses bisnis dan kinerja operasional dengan otomatisasi dan pengoptimalan berdasarkan data.

Pengembangan Produk dan Layanan Baru: Inovasi produk berbasis IoT dan layanan baru berdasarkan IoT dapat menciptakan nilai tambah dan membuka peluang bisnis yang baru.

Analitik Data dan Kecerdasan Buatan (AI): Pemanfaatan data IoT untuk pengambilan keputusan yang lebih cerdas dan integrasi kecerdasan buatan dapat meningkatkan fungsionalitas dan performa perangkat IoT.

Peningkatan Pengalaman Pengguna: Personalisasi dan kemudahan penggunaan melalui IoT dapat meningkatkan interaksi pengguna dengan lingkungannya.

12.6.2 Implikasi dan Saran untuk Pengembangan Lebih

Lanjut:

Untuk mengoptimalkan potensi IoT dan mengatasi tantangan yang dihadapi, ada beberapa implikasi dan saran yang perlu dipertimbangkan:

Keamanan dan Privasi: Pengembang dan produsen IoT harus memprioritaskan keamanan dan privasi sebagai bagian integral dari desain dan pengembangan perangkat. Pembaruan perangkat lunak rutin harus diterapkan untuk mengatasi kerentanan keamanan.

Standarisasi dan Kompatibilitas: Industri perlu bekerja sama untuk mencapai kesepakatan tentang standar dan protokol yang seragam untuk meningkatkan interoperabilitas perangkat IoT.

Efisiensi Energi: Inovasi dalam desain perangkat IoT yang hemat energi dan pengelolaan sumber daya yang efisien dapat memperpanjang masa pakai baterai dan mengurangi dampak lingkungan.

Infrastruktur dan Keterhubungan: Investasi dalam infrastruktur yang skalabel dan teknologi jaringan terbaru dapat meningkatkan keterhubungan dan responsivitas perangkat IoT.

Regulasi dan Kepatuhan: Dukungan dari regulator dan kepatuhan terhadap regulasi dan kebijakan terkait dapat menciptakan lingkungan yang aman dan mendukung perkembangan IoT.

Pengembangan SDM: Mengembangkan tenaga kerja yang memiliki keahlian dalam IoT dan keamanan siber menjadi kunci untuk menghadapi tantangan teknologi ini.

Dengan mengambil langkah-langkah strategis dan kolaboratif untuk mengatasi tantangan dan memanfaatkan peluang, masa depan IoT dapat membawa dampak yang signifikan dalam berbagai aspek kehidupan manusia, mendorong inovasi teknologi, dan menciptakan lingkungan yang lebih cerdas, efisien, dan berkelanjutan.

DAFTAR PUSTAKA

- Atzori, L., Iera, A., & Morabito, G. 2010. The Internet of Things: A survey. *Computer Networks*, 54(15), 2787-2805.
- Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. 2015. Internet of Things: A survey on enabling technologies, protocols, and applications. *IEEE Communications Surveys & Tutorials*, 17(4), 2347-2376.
- Roman, R., Zhou, J., & Lopez, J. 2013. On the features and challenges of security and privacy in distributed Internet of Things. *Computer Networks*, 57(10), 2266-2279.
- Borgia, E. 2014. The Internet of Things vision: Key features, applications and open issues. *Computer Communications*, 54, 1-31.
- Zhang, Y., & Li, D. 2018. Internet of Things (IoT) application in transportation systems: A survey. *IEEE Transactions on Intelligent Transportation Systems*, 19(12), 3912-3928.
- Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. 2013. Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems*, 29(7), 1645-1660.
- Jin, J., Gubbi, J., Marusic, S., & Palaniswami, M. 2014. An information framework for creating a smart city through Internet of Things. *IEEE Internet of Things Journal*, 1(2), 112-121.
- Herrera, J. M. 2016. An overview of the Internet of Things for people with disabilities. *Journal of Network and Computer Applications*, 67, 120-134.
- Bandyopadhyay, D., & Sen, J. 2011. Internet of Things: Applications and challenges in technology and standardization. *Wireless Personal Communications*, 58(1), 49-69.

- Lea, R. 2016. IoT and data analytics: A partnership made in tech heaven. Computerworld UK. [Online] Available at: <https://www.computerworlduk.com/data/iot-data-analytics-partnership-made-in-tech-heaven-3648993/> (Accessed on 31st July 2023).
- Lopez, D., Gómez, Ó., & Esparza, Ó. 2018. Internet of Things in the smart city: Possible applications and challenges. *International Journal of Distributed Sensor Networks*, 14(2), 1550147718764469.
- Ray, P. P. 2016. Internet of Things for smart agriculture: Technologies, practices and future direction. *Journal of Ambient Intelligence and Humanized Computing*, 7(6), 783-798.

BIODATA PENULIS



Muhammad Rizal

Dosen di Universitas Dipa Makassar

Muhammad Rizal dilahirkan di kota Palu, Sulawesi Tengah, pada bulan Agustus 1992. Setelah menyelesaikan studi Magister Teknik Elektro di Program Pascasarjana Universitas Hasanuddin pada tahun 2019, dia bekerja sebagai seorang dosen di Universitas Dipa Makassar. Selain menjadi dosen, Rizal juga aktif sebagai penulis buku dan jurnal dengan fokus pada topik informatika. Dia juga mengembangkan keahliannya dalam bidang Internet of Things dan berhasil menerapkan beberapa karyanya, seperti implementasi cuci tangan otomatis di beberapa rumah sakit di Kota Makassar, Sulawesi Selatan.

BIODATA PENULIS



Arief Yanto Rukmana, S.T., M.M.

Mahasiswa Doktoral Universitas Pendidikan Indonesia
Dosen Perguruan Tinggi Indonesia Mandiri Bandung
Dosen Universitas Nurtanio Bandung

Penulis sebelumnya telah memegang posisi penting di sejumlah bisnis yang beroperasi pada skala nasional dan dunia. penulis saat ini berprofesi sebagai praktisi bisnis (Pemilik Perusahaan di Bidang Fashion, Kuliner dan Bisnis Digital juga sebagai seorang akademisi. Penulis mengajar di Universitas Nurtanio Bandung, dan dosen tetap di perguruan tinggi indonesia mandiri (STMIK IM & STIE STAN IM). alumni dari Program Studi Informatika (S1) Sekolah Tinggi Manajemen Informatika dan Komputer Indonesia Mandiri (STMIK IM), Program Magister Manajemen (S2) di Pasca Sarjana Universitas Widyatama dan sedang melanjutkan studi Pendidikan (S3) Program Doktoral Pendidikan Teknologi dan Vokasional di Universitas Pendidikan Indonesia. Penulis aktif sebagai pembicara dan narasumber kewirausahaan juga berdedikasi sebagai praktisi bisnis / owner / pemilik beberapa perusahaan yang bergerak pada industri food, fashion and fun. serta aktif dalam organisasi nasional maupun internasional. Penulis juga seorang profesional dalam bidang public

speaking & sebagai instruktur berpengalaman untuk sertifikasi kompetensi SKKNI BNSP Digital Marketing, Social Media Marketing dan Metodologi Pelatihan Level III, Graphic Design serta Sertifikasi Kompetensi beberapa lainnya yang diselenggarakan dinas tenaga kerja kota bandung, PT Rice INTI dan Balai Besar Pengembangan Latihan Kerja (BBPLK) Bandung. Selain itu pula penulis produktif sebagai pendamping UMKM dan pengelola Inkubator Bisnis Perguruan Tinggi Indonesia Mandiri dengan membina dan melatih / coaching, mentoring serta melakukan pendampingan bisnis UMKM untuk mahasiswa yang berminat menjadi seorang entrepreneur tangguh berdayasaing pada kancah internasional.

BIODATA PENULIS



Dr. Irmawati, S.Kom., MMSI.

Dosen Program Studi Sistem Informasi
Fakultas Teknik dan Informatika
Universitas Multimedia Nusantara

Penulis adalah dosen tetap pada Program Studi Sistem Informasi Fakultas Teknik dan Informatika Universitas Multimedia Nusantara. Menyelesaikan pendidikan S1 dan S2 pada Program Studi Sistem Informasi Universitas Gunadarma dan S3 pada departemen Teknik Elektro Universitas Indonesia. Penulis menekuni bidang keilmuan meliputi *Artificial Intelligence*, *Image Processing*, *Machine Learning*, dan *Deep Learning*.

BIODATA PENULIS



Angga Aditya Permana

Dosen Informatika

Universitas Multimedia Nusantara

Angga Aditya Permana (lahir pada Desember 1989 di Jakarta) seorang dosen full time di bidang Computer Science pada Universitas Multimedia Nusantara sejak tahun 2021, fokus penelitian pada kriptografi, steganografi serta keamanan computer, namun pada tahun 2021 sedang mendalami topik bioinformatika dan network science. Angga juga memiliki hobi yaitu touring dan juga bermain bulutangkis, saat ini sedang menjadi mahasiswa program doctoral pada IPB University. Memulai karir pertama kali sebagai Network Enginner tahun 2011 dan memulai profesinya sebagai dosen pada 2013 di kampus swasta yang ada di Jakarta, pernah juga mengajar di kampus negeri yang berada di Jakarta dan Tangerang, juga pernah di undang menjadi dosen tamu untuk mengenalkan Bioinformatika di kampus negeri di Jakarta. Terimakasih..

BIODATA PENULIS



Melissa Indah Fianty, S.Kom., MMSI

Dosen Program Studi Sistem Informasi

Fakultas Teknik dan Informatika

Universitas Multimedia Nusantara

Penulis adalah dosen tetap pada Program Studi Sistem Informasi Fakultas Teknik dan Informatika, Universitas Multimedia Nusantara. Menyelesaikan pendidikan S1 pada program studi Teknik Informatika di Bina Nusantara University dan melanjutkan S2 pada program studi Manajemen Sistem Informasi di Bina Nusantara University.

BIODATA PENULIS



Heru Saputra, S.Kom., M.Kom.

Dosen Program Studi Sistem Informasi
Fakultas Teknologi Informasi dan Industri Kreatif

Penulis lahir di Banda Aceh pada tanggal 01 Mei 1984. Penulis merupakan anak pertama dari tiga bersaudara dari pasangan Sugiwarsono dan Supiana dan sudah berkeluarga dan memiliki 1 anak dengan nama Rania Navisha Shanum dan istri bernama Ilfa Stephane. Penulis merupakan dosen tetap pada Program Studi Sistem Informasi, Fakultas Teknologi Informasi dan Industri Kreatif, Universitas Metamedia. Menyelesaikan pendidikan S1 pada Jurusan Sistem Informasi dan melanjutkan S2 pada Jurusan Sistem Informasi. Penulis menekuni beberapa bidang ilmu, seperti Blockchain, Machine Learning, VR/AR dan Artificial Intelligence. Penulis berperan aktif sebagai editor di jurnal Indonesian Journal of Computer Science (IJCS), sebagai reviewer di acara seminar nasional SENATIKA 3 dan SENATIKA 4 dan sebagai narasumber di berbagai acara seminar nasional.

BIODATA PENULIS



Fahmy Rinanda Saputri, S.T., M.Eng.

Dosen Program Studi Teknik Fisika
Fakultas Teknik dan Informatika Universitas Multimedia
Nusantara

Penulis lahir pada bulan Agustus 1993 di Cilacap. Penulis adalah dosen tetap pada Program Studi Teknik Fisika Fakultas Teknik dan Informatika, Universitas Multimedia Nusantara. Menyelesaikan pendidikan S1 pada Jurusan Teknik Fisika Universitas Gadjah Mada dan melanjutkan studi pada Program Magister Teknik Fisika Universitas Gadjah Mada. Penulis menekuni bidang instrumentasi, fisika bangunan, dan energi baru terbarukan.

BIODATA PENULIS



Suwito Pomalingo, S.Kom., M.Kom.

Dosen Program Studi Informatika Fakultas Teknik dan Informatika
Universitas Multimedia Nusantara

Penulis adalah dosen tetap pada Program Studi Informatika Fakultas Teknik dan Informatika Universitas Multimedia Nusantara. Menyelesaikan pendidikan S1 pada Jurusan Teknik Informatika dan melanjutkan S2 pada Program Magister Informatika Universitas Islam Indonesia.

Saat ini sementara menyelesaikan studi Doktorat dengan topik penelitian di bidang Security Science dengan pendekatan Deep Learning. Penulis menekuni bidang keilmuan meliputi Cyber Security, Malware Analytics, Data Science, Machine Learning, dan Deep Learning, selain itu, penulis juga memiliki beberapa serifikasi internasional di bidang Cyber Security, Digital Forensics, Data Science dan Machine Learning.

BIODATA PENULIS



Rudi Sutomo, S.Kom., M.Si., M.Kom.

Dosen Program Studi Sistem Informasi
Fakultas Teknik dan Informatika
Universitas Multimedia Nusantara

Rudi Sutomo memulai karirnya di bidang IT sebagai *IT Lecturer* di tahun 2002 dan mendalami perkembangan Software Engineering di Kampus dan IT Development di bidang Hospitality (Perhotelan), terlibat dalam beberapa Project Pembangunan Aplikasi untuk menunjang kemajuan dan kelancaran sistem IT di Hotel Novotel di Kota Palembang sebagai Asisten IT Manager. Aktif dan giat sebagai Web Developer yang berpengalaman di pembangunan di bidang Aplikasi Perkantoran dan bidang Pengembangan Website terutama Project Web Desain dan Website Development dengan terlibat dalam beberapa pembangunan project aplikasi seperti Aplikasi Visual Basic “*Work Order Multi User*” digunakan untuk seluruh Divisi dalam Hotel Novotel Palembang, Sistem Informasi Akademik (SIA) Kampus Tanri Abeng University dan Project berhubungan dengan PUSMENJAR (Pusat Asesmen dan Pembelajaran) Kemendikbud yaitu Project PUSPENDIK AKSI dan beberapa Project Minor lainnya.

Beliau juga aktif berpartisipasi dalam workshop mengenai Pembuatan website baik di sekolah maupun di masyarakat dan beberapa kali dipercaya sebagai Narasumber salah satunya di “Pelatihan Pengenalan dan Pembangunan Website” di Sekolah SMKN 43 Jakarta Tahun 2019. Pada Event Penghargaan Website Tingkat Nasional diberi kepercayaan sebagai Juri pada IWA (Indonesia Website Awards) Penilaian periode Tahun 2018 dan 2019.

BIODATA PENULIS



Risanto Darmawan, MM, MKom.

Dosen Program Studi Teknik Infomatika
Fakultas Teknik, Universitas Krisnadwipayana

Penulis lahir di Jakarta, Januari 1967. Penulis menamatkan pendidikan Diploma D2 Informatika di Fakultas Politeknik Pertanian IPB Bogor di 1991. Program Sarjana (S1) di Universitas Budi Luhur, Jakarta, Fakultas Teknologi Informasi, Sistem Informasi di 2000 dan Universitas Terbuka, Tangerang Selatan, Fakultas Ekonomi, Prodi Manajemen di 2003. Penulis juga menyelesaikan program Pasca Sarjana (S2) di Universitas Pelita Harapan, Karawaci, Fakultas Business & Management, spesialisasi Marketing di 2003 dan di Sekolah Pascasarjanam, IPB Bogor, Program Studi Ilmu Komputer, di tahun 2006.

BIODATA PENULIS



Iwan Adhicandra, S.T., M.Sc.
Dosen Program Studi Informatika
Universitas Bakrie

Penulis lahir di Jakarta tanggal 1 Desember 1974. Penulis adalah dosen tetap pada Program Studi Informatika, Fakultas Teknik dan Ilmu Komputer, Universitas Bakrie, Jakarta. Menyelesaikan pendidikan S1 pada Jurusan Teknik Elektro konsentrasi bidang Teknik Telekomunikasi di Universitas Trisakti, Jakarta, dan melanjutkan S2 pada Jurusan Teknik Elektro konsentrasi bidang Komunikasi Data di University of Sheffield, Inggris. Penulis adalah Senior Member di Institute of Electrical and Electronic Engineers (SMIEEE).