CV REY MEDIA GRAFIKA

INTERNET OF THING

Kurniati, S.Kom., M.Kom
Dr. Ir. N. Tri S. Saptadi, S.Kom., MT., MM., IPM
Victor Benny Alexsius Pardosi, S.Kom., M.Sc
Dwi Sukma Donoriyanto, ST., MT
Ir. Muhammad Azhar Irwansyah, ST., M.Eng
Dr. Ismarina, S.Si.T, Bd., M.Kes
Ade Suparman, S.SI., M.Kom
Alex Copernikus Andaria, S.T., M.Pd
Dr. Ir. Masduki Zakarijah, M.T
Dr. Ilham, ST., MT

INTERNET OF THING

Penulis:
Kurniati, S.Kom., M.Kom
Dr. Ir. N. Tri S. Saptadi, S.Kom., MT., MM., IPM
Victor Benny Alexsius Pardosi, S.Kom., M.Sc
Dwi Sukma Donoriyanto, ST., MT
Ir. Muhammad Azhar Irwansyah, ST., M.Eng
Dr. Ismarina, S.Si.T, Bd., M.Kes
Ade Suparman, S.SI., M.Kom
Alex Copernikus Andaria, S.T., M.Pd
Dr. Ir. Masduki Zakarijah, M.T
Dr. Ilham, ST., MT

CV.REY MEDIA GRAFIKA
PUBLISHER

INTERNET OF THING

Penulis :
Kurniati, S.Kom., M.Kom
Dr. Ir. N. Tri S. Saptadi, S.Kom., MT., MM., IPM
Victor Benny Alexsius Pardosi, S.Kom., M.Sc
Dwi Sukma Donoriyanto, ST., MT
Ir. Muhammad Azhar Irwansyah, ST., M.Eng
Dr. Ismarina, S.Si.T, Bd., M.Kes
Ade Suparman, S.SI., M.Kom
Alex Copernikus Andaria, S.T., M.Pd
Dr. Ir. Masduki Zakarijah, M.T
Dr. Ilham, ST., MT

Penyunting dan Desain Cover :
Paput Tri Cahyono

Ukuran:
x hal + 182 hal; 14,8cm x 21cm

Diterbitkan Oleh :

CV.REY MEDIA GRAFIKA
PUBLISHER

Jln.Melati, BKG. Palapa, Blok.T No.6
Batam - Indonesia 29432
Email : reymediagrafika.rgm@gmail.com

ISBN : 978-623-8609-56-7
IKAPI: 010/Kepri/2022
Terbitan: Oktober 2024

KATA PENGANTAR

Syukur *alhamdulillah* penulis haturkan kepada Allah Swt. yang senantiasa melimpahkan karunia dan berkah-Nya sehingga penulis mampu merampungkan karya ini tepat pada waktunya, sehingga penulis dapat menghadirkannya dihadapan para pembaca. Kemudian, tak lupa *shalawat* dan salam semoga senantiasa tercurah limpahkan kepada Nabi Muhammad SAW, para sahabat, dan ahli keluarganya yang mulia.

IoT merupakan salah satu inovasi teknologi yang menghubungkan dunia digital dan fisik, memungkinkan perangkat-perangkat untuk saling berkomunikasi melalui jaringan internet. Dari sistem rumah pintar hingga aplikasi industri, *IoT* terus berkembang dan memberikan dampak signifikan dalam efisiensi, produktivitas, serta cara hidup manusia. Melalui buku ini, kami ingin memberikan pemahaman mendalam mengenai bagaimana *IoT* bekerja, potensi penerapannya, serta tantangan yang dihadapinya di masa mendatang.

Buku ini diharapkan dapat menjadi referensi yang berguna bagi mahasiswa, praktisi, dan siapa saja yang tertarik untuk memahami lebih jauh tentang *IoT*. Kami berusaha menyajikan materi dengan bahasa yang

mudah dipahami namun tetap mengedepankan aspek teknis dan ilmiah agar pembaca dapat memperoleh gambaran yang jelas dan aplikatif.

Penulis menyampaikan terima kasih yang tak terhingga bagi semua pihak yang telah berpartisipasi. Terakhir seperti kata pepatah bahwa" Tiada Gading Yang Tak Retak" maka penulisan buku ini juga jauh dari kata sempurna, oleh karena itu penulis sangat berterima kasih apabila ada saran dan masukkan yang dapat diberikan guna menyempurnakan buku ini di kemudian hari.

2024

Penulis

DAFTAR ISI

KATA PENGANTAR ..... **iii**

DAFTAR ISI ..... **v**

BAB I KOMPONEN *INTERNET OF THINK* (*IOT*) **1**

1.1. Pendahuluan 1

1.2. Sejarah Dan Perkembangan *IoT* 4

1.3. Pentingnya *IoT* di Era Digital 9

1.4. Pentingnya Memahami Komponen *IoT* 13

BAB II TEKNOLOGI PENDUKUNG *IOT* **17**

2.1. Pengantar 17

2.2. Sensor dan Aktuator 19

2.3. Komunikasi Nirkabel 22

2.4. Komputasi *Edge* dan *Fog* 24

2.5. *Cloud Computing* 26

2.6. Keamanan *IoT* 28

2.7. Protokol *IoT* 29

2.8. *Platform IoT* 31

2.9. Analisis Data dan AI 33

2.10. Kesimpulan 34

BAB III PROTOKOL KOMUNIKASI *IOT* **37**

3.1. Jenis-Jenis Protokol Komunikasi *IoT* 37

3.2. MQTT (*Message Queuing Telemetry Transport*) 40

3.3. CoAP (*Constrained Application Protocol*) 43

3.4. Protokol HTTP (*HyperText Transfer Protocol*) dalam *IoT* 46

3.5. Keamanan pada Protokol *IoT* 48

BAB IV TEKNOLOGI *NETWORK IOT* 53

4.1. Konsep Dasar Jaringan *IoT* (*Internet of Things*) 53

4.2. Teknologi Jaringan *IoT* Berbasis Koneksi Nirkabel..... 55

4.3. Teknologi Jaringan *IoT* Berbasis Koneksi Jarak Jauh..... 59

4.4. Teknologi Jaringan *IoT* Berdasarkan Koneksi Kabel..... 63

4.5. Tantangan dalam Teknologi Jaringan *IoT* ... 65

BAB V *INTEROPERABILITAS IOT* 69

5.1. Konsep Dasar Interoperabilitas *IoT*..... 69

5.2. Model Interoperabilitas dalam *IoT*..... 71

5.3. Keamanan dan Privasi dalam Interoperabilitas *IoT*..... 75

5.4. Implementasi Interoperabilitas *IoT* di Berbagai Industri..... 81

BAB VI *PLATFORM IOT* 85

6.1. Komponen Utama Platform *IoT*..... 85

6.2. Arsitektur Platform *IoT*..... 87

6.3. Fungsi Utama Platform *IoT*..... 91

6.4. Jenis-Jenis *Platform IoT*..... 94

BAB VII FUNDAMENTAL *CLOUD* 101

7.1. Definisi *Cloud Computing* 101

7.2. Model Layanan *Cloud Computing*.....101

7.3. Model Penyebaran *Cloud Computing* 104
7.4. Kinerja dan Skalabilitas *Cloud Computing* 107
7.5. Manajemen dan Pengelolaan *Cloud* 110
BAB VIII SENSOR *CLOUD*..... 115
8.1. Pengantar Sensor *Cloud* 115
8.1.1. Definisi Sensor *Cloud* 115
8.1.2. Peran dan Signifikansi dalam *IoT*..... 116
8.1.3. Manfaat dan Tantangan Implementasi Sensor *Cloud* 118
8.2. Arsitektur Sensor *Cloud* 120
8.2.1. Komponen Utama dalam Arsitektur Sensor *Cloud* 120
8.2.2. Lapisan dalam Arsitektur Sensor *Cloud* 122
8.2.3. Integrasi Sensor dengan *Cloud*: Protokol dan Teknologi 125
8.3. Fungsi dan Fitur Sensor *Cloud*..... 126
8.3.1. Pengumpulan Data dari Sensor 127
8.3.2. Penyimpanan dan Pemrosesan Data di *Cloud* 127
8.3.3. Analitik Data dalam Sensor *Cloud*..... 128
8.3.4. Pengelolaan dan Kontrol Sensor melalui *Cloud* 129
8.3.5. Keamanan dan Privasi dalam Sensor *Cloud* 130
8.4. Teknologi Pendukung Sensor *Cloud*..... 130
8.4.1. Teknologi Komputasi Awan (*Cloud Computing*)..... 131

8.4.2. Teknologi *Edge* dan *Fog Computing* dalam Sensor *Cloud* 132
8.4.3. *Platform IoT* berbasis Sensor *Cloud* 132
8.5. Implementasi dan Kasus Penggunaan Sensor *Cloud* 135
8.5.1. Implementasi Sensor *Cloud* dalam Sektor Industri 135
8.5.2. Sensor *Cloud* di Bidang Pertanian (*Smart Agriculture*) 136
8.5.3. Sensor *Cloud* di Bidang Kesehatan (*Healthcare IoT*) 137
8.5.4. Sensor *Cloud* dalam Sistem Pemantauan Lingkungan (*Environmental Monitoring*) 137
8.5.5. Sensor *Cloud* untuk *Smart City* 138
8.6. Keamanan dan Privasi dalam Sensor *Cloud* 139
8.6.1. Tantangan Keamanan pada Sensor *Cloud* 139
8.6.2. Mekanisme Keamanan untuk Perlindungan Data 141
8.6.3. Privasi Data Sensor di *Cloud* 142
8.6.4. Studi Kasus Ancaman Keamanan pada Sensor *Cloud* 144
BAB IX INDUSTRIAL *IOT* 147
9.1. Konsep Dasar Industrial *IoT* 147
9.2. Teknologi Kunci dalam Industrial *IoT* 150
9.3. Standar dan Regulasi Industrial *IoT* (I*IoT*) 155
BAB X KASUS *IOT* 161

10.1. Kasus *IoT* dalam Sektor Kesehatan 161
10.2. Kasus *IoT* dalam Sektor Transportasi 163
10.3. Kasus *IoT* dalam *Smart Cities* 165
10.4. Kasus *IoT* dalam Industri Manufaktur..... 167
10.5. Kasus *IoT* dalam Pertanian 169
10.6. Kasus *IoT* dalam *Retail* dan *E-Commerce* .. 171
DAFTAR PUSTAKA 175

BAB I
KOMPONEN *INTERNET OF THINK* (*IOT*)

1.1. Pendahuluan

Perkembangan teknologi yang cepat telah mempengaruhi proses industri, memicu revolusi industri yang memberikan karakteristik khusus pada setiap zamannya. Hingga tahun 2020, beberapa era revolusi industri telah terjadi, dimulai dari industri 1.0, 2.0, 3.0, hingga kini memasuki era industri 4.0 (Budiyanti, 2021). Perkembangan ini juga mempengaruhi kebiasaan dan cara hidup masyarakat, yang kini berada di era society 5.0, di mana teknologi internet atau *Internet of Things* (*IoT*) semakin sering digunakan dalam kehidupan sehari-hari. Pada masa ini, banyak aktivitas dapat dilakukan secara remote atau jarak jauh dengan dukungan internet.

Internet of Things (*IoT*) adalah sebuah konsep yang memungkinkan perangkat fisik yang terhubung ke Internet untuk mengumpulkan, berbagi, dan memproses data, serta berkomunikasi dan berkolaborasi tanpa interaksi manusia secara langsung (IBM, 2024). *IoT* menawarkan metode koneksi yang efektif, memungkinkan konektivitas universal untuk

siapa saja, kapan saja, di mana saja, dengan berbagai jenis layanan dan jaringan (Wibowo, 2023). *IoT* mendorong teknologi generasi berikutnya, berdampak signifikan pada strategi bisnis, dan mendukung identifikasi objek yang lebih cerdas. Perangkat *IoT* mengubah infrastruktur dan arsitektur dasar internet saat ini, memberikan berbagai manfaat yang lebih luas. *IoT* melibatkan berbagai perangkat seperti sensor, aktuator, dan perangkat *edge* yang terhubung satu sama lain melalui jaringan dan protokol komunikasi. Sensor mengumpulkan data dari lingkungan fisik, seperti suhu, kelembapan, dan cahaya, dan mengubahnya menjadi sinyal yang dapat diproses oleh perangkat lain. Aktuator melakukan tindakan fisik berdasarkan perintah yang diterima dari sistem *IoT*, seperti menyalakan lampu atau menggerakkan motor. Perangkat *edge*, seperti *mikrokontroler* dan *mikroprosesor*, memproses data dari *sensor* sebelum mengirimkannya ke *Cloud* atau pusat data, mengurangi latensi dan beban jaringan serta memungkinkan *respons* yang lebih cepat terhadap data yang dikumpulkan.

IoT mentransmisikan data menggunakan berbagai protokol komunikasi seperti MQTT, CoAP, dan HTTP, serta teknologi jaringan seperti Wi-Fi, *Bluetooth*, *Zigbee*,

LoRaWAN, dan 5G untuk komunikasi jarak pendek dan jauh. *Gateway IoT* berfungsi sebagai penghubung antara perangkat *IoT* dan jaringan yang lebih besar, mengumpulkan data dari berbagai perangkat, melakukan pra-pemrosesan, dan mengirim data ke *Cloud* untuk analisis lebih lanjut. *Cloud* menyediakan sumber daya komputasi yang luas untuk penyimpanan dan analisis data skala besar. Layanan seperti *AWS IoT*, *Google Cloud IoT*, dan *Microsoft Azure IoT* menyediakan *platform* untuk manajemen perangkat, analisis data, dan pembuatan aplikasi *IoT*. Keamanan data dan perangkat sangat penting, meliputi enkripsi data, autentikasi perangkat, serta manajemen identitas dan akses. Data yang diperoleh dari perangkat *IoT* dianalisis untuk menghasilkan wawasan yang berguna, dengan teknologi *big data* dan *machine learning* digunakan untuk mengenali pola dan tren guna membantu pengambilan keputusan.

IoT memungkinkan otomatisasi dan kontrol yang lebih efisien dalam berbagai aplikasi seperti layanan kesehatan, pertanian, transportasi, rumah pintar, kota pintar, dan industri (Wibowo, 2021). Misalnya, dalam bidang medis, perangkat *IoT* dapat memantau kondisi pasien secara langsung dan menyediakan data kepada dokter untuk diagnosis yang lebih tepat. Di bidang

pertanian, sensor *IoT* memantau kondisi tanah dan cuaca untuk membantu petani mengelola lahan mereka dengan lebih efisien. Secara keseluruhan, konsep *IoT* memiliki potensi besar untuk meningkatkan efisiensi, produktivitas, dan kualitas hidup di berbagai bidang kehidupan.

1.2. Sejarah Dan Perkembangan *IoT*

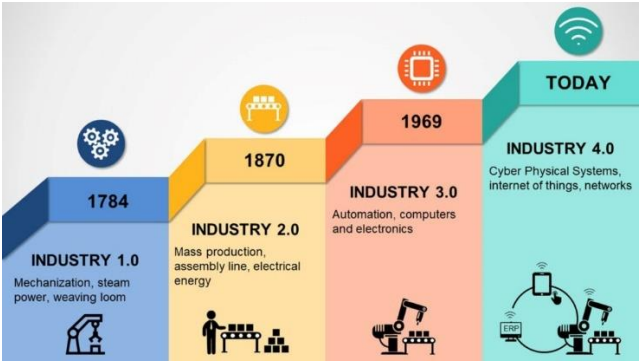
Konsep *Internet of Things* (*IoT*) pertama kali muncul pada tahun 1982 ketika sebuah mesin minuman Coca-Cola di Carnegie Mellon University menjadi perangkat pertama yang terhubung ke *internet*. Mesin ini dilengkapi dengan sensor yang dapat melaporkan inventaris dan suhu minuman dingin, memungkinkan mahasiswa dan staf untuk memeriksa ketersediaan minuman tanpa harus mendekati mesin tersebut. Inovasi ini menandai awal dari ide menghubungkan perangkat fisik ke *internet* untuk mengumpulkan dan berbagi data. Istilah "*Internet of Things*" sendiri baru diciptakan oleh Kevin Ashton pada tahun 1999 saat bekerja di Procter & Gamble(Ferdiansyah Zulkifli, 2022). Ashton menggunakan istilah ini dalam konteks presentasinya tentang penggunaan teknologi RFID (*Radio Frequency Identification*) untuk mengoptimalkan manajemen

rantai pasokan perusahaan. RFID memungkinkan identifikasi dan pelacakan otomatis objek dengan menggunakan gelombang radio, yang menjadi fondasi penting bagi pengembangan *IoT*. Pada awal 2000-an, teknologi RFID mulai diterapkan secara luas dalam berbagai industri, termasuk ritel, logistik, dan manufaktur, yang memperkuat gagasan bahwa perangkat fisik dapat berkomunikasi melalui jaringan, meletakkan dasar bagi perkembangan *IoT* yang lebih luas.

Seiring dengan perkembangan teknologi jaringan dan konektivitas, *IoT* semakin berkembang pesat. Munculnya teknologi nirkabel seperti Wi-Fi, *Bluetooth*, dan teknologi seluler 3G, 4G, dan akhirnya 5G, membuka jalan bagi semakin banyak perangkat untuk terhubung ke *internet*. Pada tahun 2008, jumlah perangkat yang terhubung ke internet melebihi jumlah populasi manusia di dunia, menandakan titik balik penting dalam perkembangan *IoT*. Pada dekade 2010-an, kemajuan dalam *big data* dan *Cloud computing* memberikan dorongan signifikan bagi *IoT*. Kemampuan untuk menyimpan, memproses, dan menganalisis data dalam skala besar memungkinkan pengembangan aplikasi *IoT* yang lebih canggih dan efektif. *Platform Cloud* seperti *AWS IoT*, *Google Cloud IoT*, dan *Microsoft*

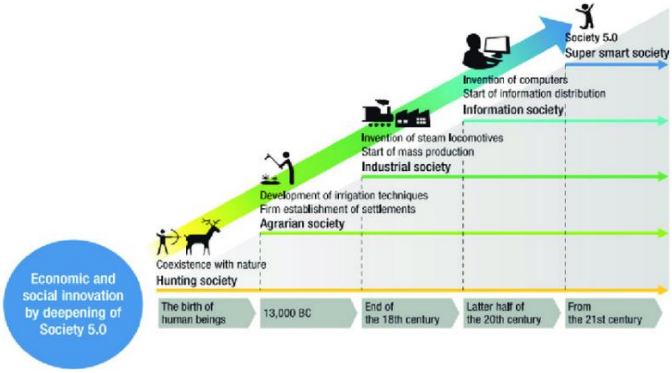
Azure IoT menyediakan infrastruktur yang diperlukan untuk manajemen perangkat, analisis data, dan pengembangan aplikasi *IoT*. Hal ini memungkinkan perusahaan dan individu untuk mengimplementasikan solusi *IoT* dengan lebih mudah dan efisien. Industri 4.0, yang dimulai pada dekade 2010-an, mengintegrasikan teknologi *IoT* dengan otomatisasi, analitik, dan kecerdasan buatan (AI) untuk menciptakan pabrik pintar.

Sebelum membahas era 4.0, kita perlu melihat kembali perkembangan era industri sebelumnya. Era 1.0 ditandai dengan penemuan mesin uap yang mulai digunakan dalam industri, menandai peralihan dari pekerjaan manual ke bantuan mesin. Era 2.0 muncul dengan teknologi kelistrikan, memungkinkan produksi massal dan lebih cepat, sehingga barang menjadi lebih murah. Pada era 3.0, industri mulai menggunakan robot dan komputer, yang meningkatkan sistematisasi dan efisiensi produksi melalui pemrograman dan pengendalian otomatis. Saat ini, kita berada di era 4.0, yang melibatkan penggunaan internet dalam berbagai aspek industri dan kehidupan, termasuk bidang kesehatan. Dengan teknologi *IoT*, kontrol jarak jauh menjadi mungkin, memungkinkan aktivitas yang tidak dibatasi oleh ruang dan waktu.



Gambar 1. *Timeline* Perkembangan Revolusi Industri

IoT menjadi inti dari revolusi industri ini, memungkinkan perangkat dan mesin untuk berkomunikasi dan beroperasi secara otomatis dengan sedikit intervensi manusia, meningkatkan efisiensi produksi, mengurangi biaya operasional, dan memungkinkan perawatan prediktif. Pada akhir dekade 2010-an dan awal 2020-an, konsep *Society* 5.0 diperkenalkan di Jepang, menggambarkan masyarakat yang menggabungkan teknologi canggih dengan kehidupan sehari-hari, di mana *IoT* memainkan peran kunci.



Gambar 2. *Timeline* Perkembengan Era Society 5.0

Pada era *society* 1.0, manusia hidup dengan berburu dan meramu serta menjalani kehidupan nomaden. Di era *society* 2.0, masyarakat mulai menetap dan bercocok tanam. Pada era *society* 3.0, industri mulai dikenal, dan pada *society* 4.0, fokus beralih pada informasi. Di era industri 4.0, masyarakat beralih ke era *society* 5.0, yaitu masyarakat cerdas yang akrab dengan *internet*, *big data*, dan kecerdasan buatan. Dalam era *society* 5.0, teknologi *internet* atau *IoT* semakin sering digunakan dalam kehidupan sehari-hari, memungkinkan banyak aktivitas dilakukan secara *remote* atau jarak jauh dengan dukungan internet, seperti *telemedicine*, pendidikan daring, dan otomatisasi rumah.

Perkembangan *IoT* terus berlanjut dengan

munculnya teknologi 5G, yang menawarkan kecepatan tinggi dan latensi rendah, memungkinkan lebih banyak perangkat terhubung secara *real-time*. Peningkatan keamanan *IoT* dan pengembangan standar interoperabilitas menjadi fokus utama untuk memastikan pertumbuhan yang berkelanjutan. Masa depan *IoT* diperkirakan akan mencakup lebih banyak aplikasi dalam berbagai sektor, dari kesehatan dan pertanian hingga transportasi dan energi, membawa dunia lebih dekat ke ekosistem yang sepenuhnya terhubung dan cerdas. Sejarah dan perkembangan *IoT* menunjukkan bagaimana teknologi ini telah berevolusi dari konsep dasar menjadi bagian integral dari kehidupan modern. Dengan dukungan konektivitas yang terus meningkat, analitik data, dan kecerdasan buatan, *IoT* memiliki potensi besar untuk terus mengubah berbagai aspek kehidupan dan industri di masa depan.

1.3. Pentingnya *IoT* di Era Digital

Internet of Things (*IoT*) memiliki peran yang sangat penting di era digital karena memungkinkan perangkat fisik dan sistem digital untuk saling terhubung dan berinteraksi secara cerdas. Kemampuan *IoT* untuk mengumpulkan, menganalisis, dan berbagi data secara

real-time membawa perubahan signifikan dalam berbagai sektor, meningkatkan efisiensi operasional dan mengoptimalkan penggunaan sumber daya di berbagai bidang, termasuk manufaktur, transportasi, kesehatan, dan pendidikan(Cholilalah, Rois Arifin, 2019). Dalam bidang kesehatan, *IoT* memungkinkan pemantauan pasien dari jarak jauh melalui perangkat medis yang terhubung. Data medis dapat dikumpulkan dan dianalisis secara terus-menerus, memungkinkan dokter untuk melakukan diagnosis lebih akurat dan merespons kondisi pasien dengan cepat. Contoh penerapannya termasuk monitor jantung yang dapat melaporkan ritme jantung secara *real-time* atau alat pemantau glukosa yang membantu penderita diabetes mengelola kadar gula darah mereka. Dengan demikian, kualitas perawatan meningkat dan pasien dapat menerima intervensi medis lebih tepat waktu.

Di sektor pertanian, *IoT* digunakan untuk memantau kondisi tanah, cuaca, dan tanaman. Sensor yang terhubung dapat mengukur kelembaban tanah, suhu, dan nutrisi, memungkinkan petani untuk melakukan irigasi dan pemupukan secara lebih efektif. Ini tidak hanya meningkatkan hasil panen tetapi juga mengurangi penggunaan air dan bahan kimia, menjadikan praktik pertanian lebih berkelanjutan dan

ramah lingkungan. Dalam transportasi, *IoT* membantu mengelola lalu lintas dan armada kendaraan. Sistem transportasi pintar menggunakan sensor dan kamera untuk memantau lalu lintas dan mengatur lampu lalu lintas secara dinamis untuk mengurangi kemacetan. Kendaraan yang terhubung dapat berkomunikasi satu sama lain dan dengan infrastruktur jalan, meningkatkan keselamatan dan efisiensi perjalanan. *IoT* juga memungkinkan pelacakan *real-time* untuk logistik dan pengiriman, memastikan barang tiba tepat waktu dan mengurangi biaya operasional. Di sektor industri manufaktur, *IoT* memungkinkan otomatisasi proses produksi dan pemeliharaan prediktif. Mesin yang terhubung dapat melaporkan status operasionalnya dan mendeteksi masalah sebelum terjadi kerusakan, mengurangi downtime dan biaya perbaikan. Proses produksi dapat dipantau dan dioptimalkan secara *real-time*, meningkatkan kualitas produk dan efisiensi produksi. Selain itu, *IoT* berperan penting dalam pengembangan smart cities, yang mengintegrasikan teknologi untuk meningkatkan manajemen energi, mengurangi polusi, dan meningkatkan kualitas hidup warga.

Selain itu, *IoT* berkontribusi pada pengembangan *smart cities*, sensor *IoT* digunakan untuk memantau

penggunaan listrik, air, dan gas secara efisien. Sistem pencahayaan jalan yang pintar dapat menyesuaikan intensitas cahaya berdasarkan kondisi cuaca dan lalu lintas, menghemat energi. Pengelolaan limbah juga ditingkatkan dengan sensor yang memantau tingkat penuh kontainer sampah, mengoptimalkan rute pengumpulan sampah. Di sektor bisnis, *IoT* membuka peluang untuk model bisnis baru dan layanan yang lebih responsif terhadap kebutuhan pelanggan. Perangkat rumah pintar, seperti termostat yang dapat dikendalikan dari jarak jauh atau sistem keamanan rumah yang dapat dipantau melalui smartphone, meningkatkan kenyamanan dan keamanan bagi pengguna. Bisnis dapat menggunakan data yang dikumpulkan dari perangkat *IoT* untuk memahami perilaku pelanggan dan menawarkan produk serta layanan yang lebih sesuai dengan kebutuhan mereka. Namun, dengan semua manfaat ini, keamanan dan privasi menjadi aspek kritis dalam implementasi *IoT*. Mengamankan data yang dikumpulkan dan memastikan perangkat tidak rentan terhadap serangan siber adalah prioritas utama. Teknik enkripsi, autentikasi perangkat, serta manajemen identitas dan akses sangat penting untuk melindungi integritas data dan kepercayaan pengguna.

Secara keseluruhan, memahami dan menerapkan teknologi *IoT* sangat penting untuk tetap kompetitif dan relevan di era digital yang terus berkembang. Dengan potensi yang besar untuk meningkatkan efisiensi, mengurangi biaya, dan menciptakan peluang baru, *IoT* menjadi fondasi bagi banyak inovasi masa depan yang dapat mengubah berbagai aspek kehidupan dan industri.

1.4. Pentingnya Memahami Komponen *IoT*

Memahami komponen *IoT* sangat penting karena teknologi ini kini menjadi bagian integral dari kehidupan sehari-hari dan berbagai sektor industri. *IoT* terdiri dari beberapa komponen utama yang bekerja bersama untuk menciptakan sistem yang efektif dan efisien diantaranya adalah:

1. **Perangkat fisik**, seperti sensor dan aktuator, adalah elemen dasar dari *IoT*. Sensor mengumpulkan data dari lingkungan, seperti suhu, kelembaban, atau gerakan, sedangkan aktuator melakukan tindakan berdasarkan data yang diterima, seperti menghidupkan lampu atau mengatur suhu. Memahami cara kerja perangkat ini memungkinkan kita untuk memilih dan menerapkan solusi yang tepat

untuk berbagai aplikasi, dari pemantauan kesehatan hingga otomatisasi rumah.

2. **Jaringan komunikasi** memungkinkan perangkat-perangkat ini untuk terhubung dan saling berinteraksi. Teknologi seperti Wi-Fi, *Bluetooth*, Zigbee, LoRaWAN, dan 5G masing-masing memiliki kelebihan dan kekurangan terkait jangkauan, konsumsi daya, dan kecepatan transmisi data. Memahami teknologi jaringan yang tersedia dan bagaimana memilih yang sesuai sangat penting untuk memastikan bahwa sistem *IoT* dapat beroperasi secara handal dan efisien.
3. ***Platform Cloud*** menyediakan infrastruktur yang diperlukan untuk menyimpan, memproses, dan menganalisis data yang dikumpulkan oleh perangkat *IoT*. Layanan seperti AWS *IoT*, Google *Cloud IoT*, dan Microsoft Azure *IoT* menawarkan solusi untuk manajemen perangkat, analisis data, dan pengembangan aplikasi. Memahami fitur dan kemampuan platform *Cloud* ini membantu dalam merancang sistem *IoT* yang skalabel dan aman, serta memastikan bahwa data dapat diakses dan digunakan secara optimal.

4. **Aplikasi analitik** memainkan peran penting dalam mengolah data yang dikumpulkan oleh perangkat *IoT*. Teknologi *big data* dan machine learning digunakan untuk mengenali pola, tren, dan wawasan dari data tersebut, yang mendukung pengambilan keputusan yang lebih baik dan lebih cepat. Mengetahui cara kerja aplikasi analitik membantu dalam memanfaatkan data secara efektif untuk meningkatkan efisiensi operasional dan hasil bisnis.
5. **Keamanan** adalah aspek kritis dalam implementasi *IoT*. Melindungi data dan perangkat dari ancaman siber memerlukan teknik enkripsi, autentikasi perangkat, serta manajemen identitas dan akses yang kuat. Memahami tantangan keamanan dan solusi yang tersedia sangat penting untuk menjaga integritas dan privasi data serta memastikan bahwa sistem *IoT* beroperasi dengan aman.

Dengan pemahaman mendalam tentang komponen-komponen ini, individu dan organisasi dapat merancang dan menerapkan solusi *IoT* yang efektif, aman, dan sesuai dengan kebutuhan spesifik

mereka. Ini juga memungkinkan mereka untuk mengatasi tantangan teknis dan operasional yang mungkin timbul, serta memaksimalkan manfaat dari teknologi *IoT* dalam berbagai aplikasi.

BAB II
TEKNOLOGI PENDUKUNG *IOT*

2.1. Pengantar

Internet of Things (*IoT*) adalah konsep revolusioner yang menghubungkan berbagai perangkat fisik ke koneksi *internet*, memungkinkan untuk mengumpulkan, mengolah, berbagi, dan mampu menganalisis data secara *real-time* (Puspita, 2024). Melalui sensor, aktuator, dan jaringan komunikasi maka perangkat ini dapat berinteraksi, berkomunikasi, dan berkolaborasi untuk menciptakan ekosistem yang cerdas dan responsif. *IoT* telah merambah berbagai sektor, mulai dari rumah pintar dan kota cerdas hingga industri manufaktur, layanan kesehatan, menghadirkan efisiensi, dan inovasi yang belum pernah ada sebelumnya.

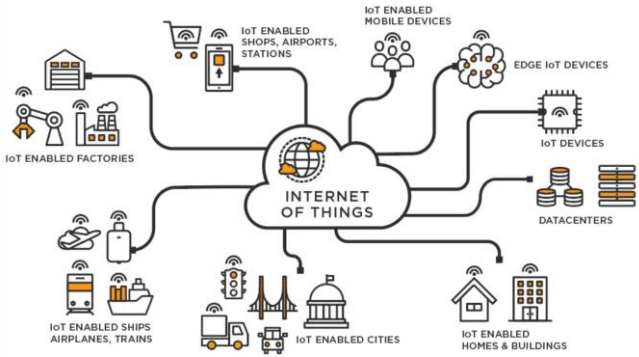
Di dunia yang semakin terhubung, *IoT* memainkan peran krusial dalam mengoptimalkan operasi dan meningkatkan kualitas hidup. Dengan mengintegrasikan perangkat yang mampu berkomunikasi satu sama lain, *IoT* memungkinkan melakukan pengawasan dan kontrol yang lebih baik terhadap berbagai aspek kehidupan manusia (Yusuf *et*

al., 2023). Misalnya, dalam rumah pintar, termostat yang terhubung dapat menyesuaikan suhu secara otomatis berdasarkan preferensi pengguna. Keberadaan kota cerdas dapat membantu sistem pengelolaan lalu lintas hingga mengurangi kemacetan dengan menyesuaikan lampu lalu lintas secara dinamis dan proporsional.

Keunggulan utama *IoT* terletak pada kemampuannya untuk menyediakan data yang kaya dan mendalam, serta dapat dianalisis untuk menghasilkan wawasan yang berharga. Data ini tidak hanya membantu dalam pengambilan keputusan yang lebih baik, tetapi juga memungkinkan prediksi dan respons yang proaktif terhadap berbagai situasi. Di sektor industri, *IoT* memungkinkan pemantauan kondisi mesin secara *real-time* sehingga dapat mencegah kerusakan dan mengurangi waktu henti dalam produksi. Bidang kesehatan membantu perangkat medis yang terhubung untuk memantau kondisi pasien secara terus-menerus dan memberikan peringatan dini terhadap potensi kesehatan.

Penerapan *IoT* juga menghadirkan tantangan, terutama dalam hal keamanan dan privasi. Dengan banyaknya perangkat yang terhubung dan bervolume data yang besar maka perlindungan terhadap ancaman

siber menjadi sangat penting (Tawalbeh *et al.*, 2020). Selain itu, standar interoperabilitas dan regulasi yang jelas diperlukan untuk memastikan bahwa perangkat dari berbagai produsen dapat bekerja sama dengan lancar. Meskipun demikian, potensi manfaat *IoT* yang besar membuatnya menjadi teknologi yang layak untuk dikembangkan dan diadopsi secara luas.



Gambar 2.1 *Internet of Things (IoT)* dan *Trend* Teknologi

Sumber: https://fakta.news/teknologi/internet-of-things-*IoT*-trend-teknologi-yang-perlu-dioptimalkan

2.2. Sensor dan Aktuator

Dalam konteks *Internet of Things* (*IoT*), sensor adalah perangkat yang mendeteksi dan mengukur perubahan fisik atau lingkungan, kemudian

mengubahnya menjadi sinyal yang dapat dianalisis oleh sistem komputer (Javaid *et al.*, 2021). Sensor memainkan peran penting dalam ekosistem *IoT* karena bertindak sebagai titik pengumpulan data yang bersifat vital. Data yang dihasilkan oleh sensor dapat mencakup berbagai aspek, seperti suhu, kelembaban, cahaya, tekanan, gerakan, dan banyak lagi. Dengan menempatkan sensor di berbagai lokasi dan objek, perangkat *IoT* dapat mengumpulkan data *real-time* yang memungkinkan pengawasan dan kontrol yang lebih akurat dan efisien.

Sensor dalam *IoT* tidak hanya pasif dalam mengumpulkan data tetapi juga sering kali dilengkapi dengan kemampuan komunikasi untuk mengirimkan data tersebut ke pusat pemrosesan atau ke perangkat lain dalam jaringan *IoT* (Bkheet and Agbinya, 2021). Hal ini memungkinkan analisis data secara langsung dan respons yang cepat terhadap kondisi yang terdeteksi. Misalnya, sensor suhu di sebuah gedung pintar dapat mengirimkan data ke sistem HVAC (*Heating*, *Ventilation*, and *Air Conditioning*) untuk menyesuaikan suhu ruangan secara otomatis. Sensor menjadi komponen kunci yang memungkinkan *IoT* mencapai suatu tujuan untuk menciptakan lingkungan yang lebih cerdas, responsif, dan terintegrasi. Terdapat

berbagai jenis sensor yang digunakan dalam *IoT* seperti sensor suhu, sensor kelembaban, sensor cahaya, sensor gerak, dan sensor *proximity*.

Aktuator dalam konteks *Internet of Things* (*IoT*) adalah perangkat yang menerima sinyal dari sistem kontrol dan kemudian melakukan tindakan fisik untuk mengubah keadaan atau lingkungan. Tindakan ini bisa berupa menggerakkan motor, membuka atau menutup katup, menghidupkan atau mematikan lampu, atau bahkan mengendalikan suatu perangkat elektronik yang lain. Aktuator bertindak sebagai eksekutor dalam sistem dengan berperan untuk menerjemahkan instruksi *digital* menjadi tindakan nyata yang dapat mempengaruhi dunia fisik. Aktuator berkemampuan untuk memungkinkan interaksi dinamis antara perangkat *IoT* dan lingkungan sekitar dan memberikan kemampuan untuk melakukan tugas otomatis yang sebelumnya memerlukan intervensi manusia.

Peran aktuator dalam *IoT* sangat penting karena memungkinkan sistem untuk tidak hanya mengumpulkan dan menganalisis data, tetapi juga untuk mengambil tindakan berdasarkan analisis tersebut. Misalnya, dalam sistem rumah pintar, aktuator dapat digunakan untuk mengatur tirai jendela secara otomatis berdasarkan intensitas cahaya yang

terdeteksi oleh sensor cahaya.

Dalam industri manufaktur, aktuator dapat mengontrol mesin untuk meningkatkan efisiensi produksi dan mengurangi kesalahan manusia. Aktuator berkemampuan membantu mewujudkan visi *IoT* untuk menciptakan lingkungan yang lebih otomatis, efisien, dan responsif terhadap perubahan yang terjadi secara *real-time*. Secara umum, aktuator dalam *IoT* berupa motor, *relay*, dan pompa.

2.3. Komunikasi Nirkabel

Komunikasi nirkabel adalah teknologi yang memungkinkan pengiriman informasi antar perangkat tanpa menggunakan kabel fisik. Dalam konteks *Internet of Things* (*IoT*), komunikasi nirkabel merupakan tulang punggung yang memungkinkan perangkat *IoT* dapat terhubung, berkomunikasi, dan bertukar data secara efisien (Tan, Budiman and Skynyrd, 2023). Teknologi komunikasi nirkabel yang umum digunakan dalam *IoT* berupa *Wi-Fi*, *Bluetooth*, *Zigbee*, *LoRaWAN*, dan *5G*.

Wi-Fi adalah teknologi yang sering digunakan untuk menghubungkan perangkat dalam jaringan area lokal (*LAN*), dengan kecepatan tinggi dan jangkauan yang cukup luas (Priantama, 2017). *Bluetooth* sesuai untuk komunikasi jarak pendek dengan konsumsi daya

rendah, seperti pada perangkat *wearable* atau sensor di rumah pintar. *Zigbee* digunakan dalam aplikasi rumah pintar dan industri *IoT* dengan kebutuhan konsumsi daya yang rendah serta jangkauan yang dapat diperluas melalui pembentukan jaringan *mesh*. *LoRaWAN* menawarkan jangkauan yang jauh dengan konsumsi daya rendah dan sesuai untuk aplikasi jarak jauh seperti pemantauan pertanian atau kota cerdas.

Jaringan nirkabel adalah teknologi yang memungkinkan dua perangkat atau lebih dapat terhubung tanpa kabel. Teknologi *5G* menjanjikan kecepatan tinggi dan latensi rendah sehingga mendukung aplikasi *IoT* yang memerlukan respons cepat dan koneksi yang stabil, seperti mobil otonom atau pabrik pintar. Melalui berbagai pilihan teknologi komunikasi nirkabel ini, *IoT* dapat diimplementasikan dalam berbagai skenario dengan memperhatikan kebutuhan spesifik dari masing-masing aplikasi dan lingkungan operasional (Sugiyatno, Sidiq and Edrisy, 2024).

Gambar 2.2 Jaringan *Nirkabel*
Sumber: https://it.telkomuniversity.ac.id/contoh-jaringan-nirkabel-simak-fungsi-dan-jenisnya/

2.4. Komputasi *Edge* dan *Fog*

Komputasi *Edge* dan *Fog* merupakan paradigma dalam komputasi terdistribusi yang mendekatkan pemrosesan data dan komputasi ke ujung jaringan (*edge*) atau ke "kabut" (*fog*), di dekat sumber data atau pengguna (García-Valls, Dubey and Botti, 2018). Komputasi *Edge* mengacu pada pemrosesan data yang dilakukan di dekat perangkat atau lokasi di mana data

dihasilkan, seperti sensor *IoT* atau perangkat pintar. Hal ini memungkinkan analisis data secara *real-time* dan pengambilan keputusan yang cepat tanpa harus mengirimkan data ke pusat data jarak jauh sehingga mengurangi latensi dan memperbaiki respons sistem.

Komputasi *Fog* memperluas konsep dengan membawa komputasi, penyimpanan data, dan aplikasi lebih dekat ke perangkat *edge* dan ke titik distribusi data di dalam jaringan. *Fog computing* membantu mengatasi tantangan yang muncul dari jumlah besar data yang dihasilkan oleh perangkat *IoT* dengan menyediakan kapasitas pemrosesan dan penyimpanan di antara perangkat *edge* dan *Cloud*. Melalui upaya mengimplementasikan komputasi *Edge* dan *Fog*, maka organisasi dapat mengoptimalkan penggunaan sumber daya *IT*, meningkatkan kecepatan respons sistem, dan mengurangi biaya transmisi data dalam konteks *IoT* yang semakin berkembang pesat.

Komputasi *Edge* merujuk pada pemrosesan data yang dilakukan di atau dekat lokasi pengumpulan data, mengurangi latensi dan penggunaan *bandwidth*. Manfaat utama dari komputasi *edge*, meliputi: respons cepat dengan pemrosesan data secara lokal mengurangi waktu respon, keamanan dengan data sensitif yang dapat diproses dan disimpan secara lokal,

efisiensi *bandwidth* dengan mengurangi jumlah data yang harus dikirim ke pusat data.

Komputasi *Fog* adalah perpanjangan dari komputasi *Cloud* yang memperluas kemampuan komputasi dan penyimpanan ke *"fog"* atau lapisan yang lebih dekat perangkat *edge*. *Fog* memiliki manfaat yang meliputi: distribusi beban kerja dengan menyebarkan beban pemrosesan antara *Cloud* dan *edge*, reduksi latensi dengan menyediakan pemrosesan data yang lebih dekat dengan sumbernya, dan skalabilitas yang memungkinkan penskalaan yang lebih fleksibel sesuai kebutuhan.

2.5. *Cloud Computing*

Cloud computing adalah paradigma komputasi yang memungkinkan akses yang mudah dan fleksibel terhadap sumber daya komputasi (seperti *server*, penyimpanan data, *database*, aplikasi, dan layanan IT lainnya) melalui *internet* (Syaikhu, 2013). Dalam model ini, layanan *Cloud* disediakan oleh penyedia layanan *Cloud* besar seperti *Amazon Web Services* (*AWS*), *Microsoft Azure*, dan *Google Cloud Platform*, yang mengelola infrastruktur dan memungkinkan pengguna untuk menyewa sumber daya berdasarkan kebutuhan. Penggunaan *Cloud computing* memungkinkan

organisasi untuk mengurangi biaya investasi awal dalam infrastruktur IT, karena tidak perlu membeli atau memelihara perangkat keras fisik sendiri. Selain itu, *Cloud computing* menawarkan skalabilitas yang lebih baik sehingga memungkinkan pengguna untuk meningkatkan atau mengurangi kapasitas sumber daya sesuai dengan permintaan tanpa gangguan layanan.

Keunggulan dari pemanfaatan *Cloud computing* adalah kemudahan akses global ke data dan aplikasi, memungkinkan kolaborasi tim yang terdistribusi secara geografis dan mempercepat inovasi. Selain itu, *Cloud computing* mendukung model pengembangan perangkat lunak seperti *Software-as-a-Service* (*SaaS*), *Platform-as-a-Service* (*PaaS*), dan *Infrastructure-as-a-Service* (*IaaS*), yang dapat memungkinkan pengembang untuk fokus pada pengembangan aplikasi tanpa harus memikirkan tentang infrastruktur di balik layanan tersebut (Wiwin Hartanto, 2018). Namun, terdapat pula tantangan terkait dengan keamanan data dan privasi, terutama dalam pengelolaan data sensitif yang disimpan pada layanan *Cloud*. Meskipun demikian, *Cloud computing* tetap menjadi pilihan utama bagi banyak organisasi untuk meningkatkan efisiensi operasional, inovasi produk, dan responsivitas terhadap kebutuhan pasar yang berubah dengan cepat.

2.6. Keamanan *IoT*

Keamanan adalah aspek kritis dalam *IoT* untuk melindungi data dan perangkat dari ancaman (Najib, Sulistyo and Widyawan, 2020). Teknologi keamanan utama, meliputi: enkripsi yang mengamankan data yang ditransmisikan antara perangkat, autentikasi yang memastikan hanya pengguna dan perangkat yang sah dapat mengakses jaringan, *firewall* dan *IDS*/*IPS* yang mampu melindungi jaringan dari serangan siber, dan manajemen sertifikat *digital* untuk komunikasi yang aman.

Keamanan *IoT* menjadi perhatian utama karena jumlah perangkat terhubung yang terus bertambah di seluruh sektor dan berasal dari rumah pintar hingga infrastruktur kritis. Tantangan utama dalam keamanan *IoT* meliputi rentannya perangkat terhadap serangan jaringan, pengumpulan data pribadi yang sensitif, dan potensi penyalahgunaan akses yang tidak sah. Untuk mengatasi ini, penting dalam menerapkan praktik keamanan yang kuat, mulai dari perancangan perangkat *IoT* hingga implementasi infrastruktur jaringan. Hal yang perlu diperhatikan, meliputi penggunaan enkripsi data yang kuat, autentikasi yang ketat untuk mengelola akses perangkat, dan pembaruan perangkat lunak yang teratur untuk

mengatasi kerentanan keamanan yang ditemukan.

Pemantauan dan deteksi ancaman secara proaktif juga krusial dalam melindungi sistem *IoT*. Solusi seperti *firewall*, deteksi intrusi, dan sistem manajemen keamanan informasi (*ISMS*) dapat membantu mendeteksi, mencegah, dan merespons ancaman keamanan sebelum mengakibatkan kerusakan yang signifikan. Upaya kolaboratif antara industri, regulator, dan peneliti keamanan juga diperlukan untuk mengembangkan standar keamanan yang lebih baik dan mendorong kesadaran tentang praktik terbaik dalam pengembangan dan penggunaan perangkat *IoT*. Dengan mengadopsi pendekatan komprehensif terhadap keamanan maka akan memastikan bahwa potensi inovatif dari *IoT* dapat direalisasikan tanpa mengorbankan privasi dan keamanan pengguna.

2.7. Protokol *IoT*

Protokol komunikasi adalah aturan yang mengatur pertukaran data antara perangkat (Prastiyanto Dhidik, 2012). Beberapa protokol *IoT* utama meliputi: *MQTT* (*Message Queuing Telemetry Transport*) berupa protokol ringan untuk komunikasi antar perangkat, *CoAP* (*Constrained Application Protocol*) merupakan protokol *web* untuk perangkat yang terbatas sumber

daya, *HTTP*/*HTTPS* merupakan protokol standar untuk komunikasi *web*, dan *AMQP* (*Advanced Message Queuing Protocol*) sebagai protokol yang memberi pesan bisnis dengan kebutuhan reliabilitas tinggi.

Protokol *IoT* adalah seperangkat aturan dan standar komunikasi yang memungkinkan perangkat *IoT* untuk berkomunikasi dan berinteraksi satu sama lain, serta dengan sistem yang lain dalam infrastruktur *IoT*. Protokol ini menentukan cara perangkat mentransmisikan data, memvalidasi identitas, dan menanggapi permintaan atau perintah dari pengguna atau sistem lain. Beberapa protokol umum yang digunakan dalam *IoT* termasuk *MQTT* (*Message Queuing Telemetry Transport*), *CoAP* (*Constrained Application Protocol*), *HTTP* (*Hypertext Transfer Protocol*), dan *AMQP* (*Advanced Message Queuing Protocol*).

Pemilihan protokol *IoT* biasanya didasarkan pada kebutuhan spesifik aplikasi dan lingkungan operasionalnya. *MQTT* sering digunakan untuk aplikasi yang membutuhkan komunikasi yang ringan dan berkinerja tinggi, sementara *CoAP* sesuai untuk perangkat dengan sumber daya terbatas seperti sensor di jaringan sensor tanpa kabel. *HTTP* digunakan ketika komunikasi dengan *server web* diperlukan, seperti

dalam aplikasi yang terhubung ke *platform Cloud*. *Advanced Message Queuing Protocol* (*AMQP*) merupakan standar terbuka dalam melanjutkan pesan bisnis antar aplikasi atau organisasi. Pemahaman yang baik tentang protokol *IoT* dapat membantu dalam merancang, mengimplementasikan, dan mengelola infrastruktur *IoT* dengan efisien dan aman, memastikan interoperabilitas perangkat dan aplikasi dalam ekosistem yang semakin terhubung.

2.8. *Platform IoT*

Platform IoT menyediakan berbagai layanan untuk mendukung pengembangan, *deployment*, dan manajemen aplikasi *IoT* (Pradana and Bhawiyuga, 2022). Beberapa *platform* populer meliputi: *AWS IoT* yang merupakan *platform* dari *Amazon Web Services* untuk mengelola perangkat *IoT*, *Google Cloud IoT* yang memberikan layanan dari *Google* untuk konektivitas dan analisis data *IoT*, dan *Microsoft Azure IoT* yang merupakan *platform* dari *Microsoft* yang menyediakan layanan *IoT* yang sangat komprehensif dan proporsional.

Platform IoT merupakan infrastruktur *software* yang menyediakan berbagai layanan dan komponen untuk mendukung pengembangan, manajemen, dan

integrasi perangkat *IoT* serta data yang dihasilkan. *Platform* ini biasanya mencakup berbagai fitur, seperti manajemen perangkat (*device management*), pengumpulan data (*data collection*), analisis data (*data analytics*), keamanan (*security*), dan integrasi dengan sistem lain, seperti *Cloud computing* atau sistem *enterprise* (Anggy Giri Prawiyogi and Aang Solahudin Anwar, 2023). *Platform IoT* memungkinkan pengguna untuk mengelola perangkat *IoT* secara efisien, menganalisis data yang dikumpulkan untuk mendapatkan wawasan yang berharga, dan mengintegrasikan data ke dalam proses bisnis atau aplikasi yang lebih besar dan memiliki jangkauan luas.

Terdapat berbagai *platform IoT* yang tersedia dari penyedia besar, seperti *AWS IoT*, *Microsoft Azure IoT*, dan *Google Cloud IoT*, serta *platform open-source* seperti *Eclipse IoT* dan *ThingsBoard*. Setiap *platform* biasanya menawarkan keunggulan tertentu, seperti skalabilitas, keamanan yang ditingkatkan, atau integrasi yang mudah dengan infrastruktur *IT* yang ada (Wisnawa, Prasetia and Lahallo, 2021). Pemilihan *platform IoT* yang tepat tergantung pada kebutuhan spesifik bisnis atau aplikasi, termasuk skala proyek, kompleksitas integrasi, dan kebutuhan analisis data yang diinginkan. Dengan adopsi *platform IoT* yang

sesuai, organisasi dapat memanfaatkan potensi penuh dari perangkat *IoT*, meningkatkan efisiensi operasional, dan menciptakan nilai tambah melalui inovasi teknologi yang memungkinkan mengikuti tren perkembangan.

2.9. Analisis Data dan AI

Data yang dikumpulkan dari perangkat *IoT* dapat dianalisis untuk mendapatkan wawasan yang berharga. Analisis data dan kecerdasan buatan (*AI*) memainkan peran krusial dalam mendukung implementasi dan efektivitas (Fadillah and Gunawan, 2024). Jumlah besar data yang dihasilkan oleh perangkat *IoT* akan melalui analisis data yang menjadi kunci untuk menghasilkan wawasan yang bernilai dari informasi yang terkumpul. Teknik analisis data seperti pemrosesan *stream* data (*stream processing*), analisis prediktif, dan pemodelan statistik digunakan untuk mengekstrak pola, tren, dan informasi penting dari data *IoT*. Organisasi akan membuat keputusan lebih tepat waktu dan informatif, mengoptimalkan operasi, serta meningkatkan efisiensi dan produktivitas secara keseluruhan.

Kecerdasan buatan (*AI*) memberikan kemampuan untuk mengotomatisasi analisis data *IoT* dan mengidentifikasi pola yang lebih kompleks dan

tersembunyi. Penggunaan teknik seperti *machine learning* dan *deep learning* membuat *AI* dapat memproses data dalam skala besar dan menghasilkan prediksi yang akurat berdasarkan data historis dan *real-time*. Dalam lingkungan industri, *AI* dapat digunakan untuk memprediksi kegagalan perangkat sebelum terjadi, meningkatkan waktu operasional dan mengurangi biaya pemeliharaan. Secara keseluruhan, integrasi analisis data dan *AI* dengan *IoT* memungkinkan organisasi untuk mengoptimalkan operasional, meningkatkan pengalaman pengguna, dan menciptakan nilai tambah melalui pemahaman yang lebih baik terhadap data yang dikumpulkan.

Teknologi analisis data dan *AI* dalam *IoT*, meliputi: *machine Learning* yang merupakan algoritma yang belajar dari data untuk membuat prediksi dan keputusan, *big data analytics* yang merupakan teknologi untuk menganalisis data dalam jumlah besar dengan cepat, dan *real-time analytics* yang berfunsi menganalisis data secara langsung untuk respons cepat.

2.10. Kesimpulan

Teknologi pendukung *IoT* adalah fondasi yang memungkinkan perangkat berfungsi dengan efektif dan efisien. Dari sensor dan komunikasi nirkabel hingga

komputasi *edge* dan *Cloud*, setiap teknologi memainkan peran penting dalam ekosistem *IoT* yang terus berkembang. Memahami dan memanfaatkan teknologi ini adalah kunci untuk sukses dalam implementasi di berbagai industri.

Teknologi pendukung *IoT* seperti komputasi *edge*, *fog computing*, sensor cerdas, dan *platform* telah mengubah cara berinteraksi dengan lingkungan sekitar dan sistem di sekitar. Pemanfaatan teknologi *IoT* telah memungkinkan integrasi yang lebih mendalam antara dunia fisik dan dunia *digital*, menciptakan kesempatan baru untuk efisiensi, keamanan, dan kenyamanan. Komputasi *edge* memungkinkan pemrosesan data di lokasi di mana data dihasilkan, mengurangi latensi dan mengoptimalkan respons sistem *real-time*, sementara *fog computing* menyediakan infrastruktur yang diperlukan untuk menangani volume data yang besar yang dihasilkan oleh perangkat *IoT*.

Sensor cerdas yang terhubung dan *platform IoT* yang canggih membuat organisasi mengelola perangkat *IoT* dengan efektif, menganalisis data yang dihasilkan untuk mendapatkan wawasan yang berharga, dan mengintegrasikan solusi *IoT* ke dalam operasi dengan lebih mulus. Terdapat tantangan seperti keamanan dan interoperabilitas, perkembangan teknologi pendukung

IoT yang menginspirasi inovasi di berbagai sektor hingga rumah pintar industri 4.0. Pengembangan dan pengadopsian teknologi dapat mengharapkan masa depan yang lebih terhubung, cerdas, dan berkelanjutan.

BAB III
PROTOKOL KOMUNIKASI *IOT*

3.1. Jenis-Jenis Protokol Komunikasi *IoT*

1. Protokol Aplikasi Protokol di lapisan aplikasi memungkinkan perangkat *IoT* untuk bertukar data melalui jaringan. Berikut adalah beberapa protokol aplikasi yang umum digunakan:
    a. HTTP (Hypertext Transfer Protocol): Protokol yang biasa digunakan untuk komunikasi *web*. Dalam konteks *IoT*, HTTP kurang efisien karena konsumsi daya dan bandwidth yang tinggi, tetapi masih digunakan untuk aplikasi yang membutuhkan interaksi manusia seperti smart home.
    b. MQTT (Message Queuing Telemetry Transport): Protokol komunikasi ringan yang sangat sesuai untuk perangkat *IoT* dengan sumber daya terbatas. Dirancang untuk konektivitas di jaringan dengan latensi tinggi atau bandwidth rendah.

c. CoAP (Constrained Application Protocol): Protokol berbasis UDP yang dirancang untuk perangkat dengan sumber daya terbatas. CoAP memiliki overhead lebih kecil dibandingkan HTTP dan lebih cocok untuk aplikasi *real-time* di *IoT*.

2. Protokol Jaringan Protokol jaringan memungkinkan komunikasi antar perangkat *IoT* melalui internet atau jaringan lokal. Contoh protokol jaringan *IoT* adalah:
    a. IPv4 dan IPv6: Keduanya adalah protokol alamat IP, tetapi IPv6 dirancang untuk mengatasi keterbatasan IPv4 dalam hal ruang alamat yang lebih luas, serta menawarkan peningkatan efisiensi routing dan keamanan.
    b. 6LoWPAN (IPv6 over Low-Power Wireless Personal Area Networks): Protokol yang memungkinkan IPv6 berjalan di jaringan area pribadi nirkabel yang rendah daya, seperti Zigbee dan BLE. 6LoWPAN sangat cocok

untuk komunikasi nirkabel di perangkat dengan keterbatasan daya.

c. RPL (Routing Protocol for Low-Power and Lossy Networks): Protokol routing yang dioptimalkan untuk jaringan *IoT* yang lemah dan berdaya rendah. RPL sangat cocok untuk jaringan sensor nirkabel dan aplikasi *IoT* berskala besar.

3. Protokol Penghubung (Link *Layer*) Protokol pada lapisan penghubung bertanggung jawab untuk komunikasi langsung antar perangkat pada jaringan lokal. Protokol-protokol ini mendukung berbagai teknologi nirkabel seperti:

   a. Wi-Fi: Teknologi yang umum digunakan untuk konektivitas internet di banyak perangkat *IoT*, terutama di rumah dan kantor. Wi-Fi menawarkan kecepatan tinggi tetapi boros daya.

   b. *Bluetooth* Low Energy (BLE): Teknologi nirkabel dengan konsumsi daya rendah yang digunakan dalam perangkat jarak dekat seperti wearable dan sensor kesehatan. BLE dirancang untuk komunikasi berjangka pendek.

c. Zigbee: Protokol komunikasi nirkabel yang digunakan di perangkat dengan daya rendah dan jaringan mesh, umumnya digunakan dalam aplikasi smart home dan sistem otomatisasi industri.
d. LoRaWAN (Long Range Wide Area Network): Protokol untuk komunikasi jarak jauh pada perangkat *IoT* dengan daya sangat rendah. LoRaWAN sering digunakan di aplikasi seperti monitoring lingkungan dan jaringan kota pintar.
e. NB-*IoT* (Narrowband *IoT*): Teknologi komunikasi seluler yang dioptimalkan untuk perangkat *IoT* dengan konsumsi daya rendah dan cakupan yang luas. Cocok untuk aplikasi yang memerlukan konektivitas jarak jauh dengan data rate rendah, seperti meteran air dan listrik pintar.

3.2. MQTT (*Message Queuing Telemetry Transport*)

MQTT adalah protokol komunikasi yang ringan dan sangat populer dalam aplikasi *Internet of Things* (*IoT*). Dirancang oleh IBM pada tahun 1999, MQTT

memungkinkan perangkat yang memiliki sumber daya terbatas dan jaringan yang tidak stabil untuk mengirim dan menerima data dengan efisien. MQTT dirancang untuk aplikasi yang membutuhkan transmisi data dalam jumlah kecil dengan latensi rendah dan konsumsi bandwidth minimal.

Fitur Utama MQTT:

1. Protokol yang Ringan: MQTT menggunakan sedikit bandwidth dan memiliki overhead yang rendah, membuatnya cocok untuk perangkat *IoT* yang memiliki sumber daya terbatas, seperti sensor dan aktuator.
2. Model Komunikasi "Publish/Subscribe":
    a. Publisher: Perangkat atau aplikasi yang mengirim data (misalnya, sensor yang mengirimkan suhu).
    b. Subscriber: Perangkat atau aplikasi yang menerima data.
    c. Broker: *Server* perantara yang mengelola pesan antara publisher dan subscriber. Semua komunikasi dilakukan melalui broker, yang memastikan pesan dikirim ke subscriber yang tertarik pada topik tertentu.

3. Topik: MQTT menggunakan sistem topik untuk mengelola pesan. Setiap pesan yang dikirim memiliki topik tertentu (misalnya, "sensor/suhu/ruangan1"), dan subscriber hanya akan menerima pesan untuk topik yang mereka ikuti.
4. QoS (Quality of Service): MQTT mendukung tiga level QoS yang menentukan keandalan pengiriman pesan:
    a. QoS 0 (At most once): Pesan dikirim tanpa konfirmasi, bisa gagal.
    b. QoS 1 (At least once): Pesan dikirim minimal satu kali, memastikan pengiriman meski ada duplikasi.
    c. QoS 2 (Exactly once): Pesan dijamin sampai ke subscriber tepat satu kali, tanpa duplikasi.
5. Persistensi Koneksi: MQTT mendukung persistensi koneksi, yang berarti bahwa perangkat dapat tetap terhubung dalam waktu lama tanpa memerlukan sinkronisasi terus-menerus. Ini sangat bermanfaat dalam aplikasi *IoT* yang menggunakan daya baterai rendah.
6. Retained Messages: Pesan yang diterbitkan dapat ditandai sebagai "retained," sehingga

subscriber yang baru bergabung akan langsung mendapatkan pesan terbaru.

7. Kegunaan di Jaringan yang Tidak Stabil: MQTT bekerja baik di lingkungan dengan latensi tinggi atau jaringan yang tidak stabil, seperti jaringan seluler atau satelit.

3.3. CoAP (*Constrained Application Protocol*)

CoAP (*Constrained Application Protocol*) adalah protokol komunikasi berbasis UDP (*User Datagram Protocol*) yang dirancang khusus untuk perangkat *IoT* (*Internet of Things*) dengan sumber daya terbatas. Protokol ini dikembangkan oleh IETF (*Internet Engineering Task Force*) dalam grup kerja Constrained RESTful Environments (*CoRE*) dan dioptimalkan untuk perangkat dengan keterbatasan dalam daya, memori, dan kemampuan pemrosesan, seperti sensor, aktuator, dan kontroler yang digunakan di lingkungan *IoT*.

Fitur Utama CoAP:

1. Protokol Ringan: CoAP dirancang dengan overhead yang sangat rendah sehingga dapat digunakan pada perangkat dengan sumber daya terbatas. Ini menjadikannya pilihan yang ideal untuk perangkat *IoT* kecil dan jaringan yang lemah.

2. Model RESTful (Representational State Transfer): CoAP mengikuti prinsip REST seperti HTTP, dengan menggunakan metode seperti GET, POST, PUT, dan DELETE untuk mengakses sumber daya pada perangkat *IoT*. CoAP memungkinkan perangkat *IoT* bertindak sebagai "*server*" yang menyediakan sumber daya (seperti data sensor) dan perangkat lain atau aplikasi yang bertindak sebagai "klien" untuk mengakses sumber daya tersebut.
3. UDP (User Datagram Protocol): CoAP menggunakan UDP sebagai lapisan transportasinya, berbeda dengan HTTP yang menggunakan TCP. Dengan menggunakan UDP, CoAP dapat mengurangi latensi dan overhead dibandingkan dengan TCP, sehingga cocok untuk jaringan dengan bandwidth terbatas dan aplikasi yang memerlukan komunikasi *real-time*.
4. Reliability Mechanism: Karena UDP tidak menyediakan jaminan pengiriman pesan, CoAP menambahkan mekanisme reliabilitas, seperti:
    a. Confirmable Messages (CON): Pesan yang membutuhkan konfirmasi dari

penerima, memastikan pesan dikirim ulang jika tidak ada tanggapan.

b. Non-Confirmable Messages (NON): Pesan yang tidak membutuhkan konfirmasi dan hanya dikirim sekali tanpa pengiriman ulang.

5. URI (Uniform Resource Identifier): CoAP menggunakan URI untuk mengidentifikasi sumber daya di jaringan, mirip dengan cara kerja HTTP di *web*. Ini memungkinkan klien untuk mengakses sumber daya menggunakan alamat unik.
6. Observasi dan Subskripsi: CoAP memungkinkan klien untuk berlangganan pembaruan terhadap sumber daya tertentu. Ketika nilai suatu sumber daya berubah (misalnya, data dari sensor), *server* CoAP dapat memberi tahu klien yang berlangganan secara otomatis, tanpa memerlukan polling terus-menerus.
7. Security: CoAP mendukung keamanan melalui penggunaan DTLS (Datagram Transport *Layer* Security), yang memberikan enkripsi, otentikasi, dan integritas data, serupa dengan SSL/TLS pada TCP.

3.4. Protokol HTTP (*HyperText Transfer Protocol*) dalam *IoT*

HTTP (*HyperText Transfer Protocol*) adalah protokol komunikasi yang umum digunakan untuk mengirimkan data di *web*. Meskipun HTTP pada awalnya tidak dirancang untuk perangkat *Internet of Things* (*IoT*), protokol ini tetap digunakan dalam beberapa aplikasi *IoT* karena sifatnya yang sudah mapan, familiar, dan mendukung interaksi berbasis REST (*Representational State Transfer*).

Fitur Utama HTTP dalam *IoT*:

1. Model Client-*Server*: HTTP mengikuti arsitektur client-*server*. Klien (seperti perangkat *IoT*) membuat permintaan ke *server* yang mengelola dan menyimpan data. Ini memungkinkan perangkat *IoT* mengakses sumber daya melalui metode HTTP standar seperti GET, POST, PUT, dan DELETE.
2. Protokol Berbasis Teks: HTTP adalah protokol berbasis teks yang mudah dipahami dan diimplementasikan. Namun, ini juga menghasilkan overhead yang lebih besar dibandingkan dengan protokol yang dioptimalkan untuk *IoT* seperti MQTT atau

CoAP, terutama karena HTTP membawa banyak metadata dalam setiap pesan.

3. Stateless (Tanpa Status): HTTP bersifat stateless, yang berarti bahwa setiap permintaan antara klien dan *server* diproses secara independen, tanpa memerlukan informasi tentang sesi sebelumnya. Ini membuat HTTP mudah diimplementasikan, tetapi kurang efisien dalam aplikasi *IoT* yang memerlukan koneksi berkelanjutan dan komunikasi berulang.
4. RESTful API: HTTP digunakan secara luas untuk RESTful API dalam *IoT*. REST (Representational State Transfer) adalah pendekatan yang memungkinkan perangkat *IoT* untuk mengakses sumber daya yang diwakili sebagai URL. Setiap sumber daya dapat dimanipulasi melalui permintaan HTTP seperti GET (untuk membaca data), POST (untuk membuat data), PUT (untuk memperbarui data), dan DELETE (untuk menghapus data).
5. HTTP/2: Versi terbaru dari HTTP, yaitu HTTP/2, memperkenalkan berbagai peningkatan, seperti multiplexing (mengirimkan beberapa permintaan sekaligus) dan pengurangan overhead header. Ini dapat

membuat HTTP lebih efisien di lingkungan *IoT* yang memerlukan koneksi lebih responsif dan cepat.

3.5. Keamanan pada Protokol *IoT*

Keamanan pada protokol *IoT* sangat penting karena perangkat *IoT* sering kali terhubung ke jaringan terbuka atau publik yang rentan terhadap serangan. Ada berbagai ancaman seperti penyadapan, modifikasi data, serangan denial-of-service (DoS), serta pencurian identitas perangkat. Setiap protokol komunikasi *IoT* memiliki mekanisme dan tantangan tersendiri dalam hal keamanan. Berikut ini beberapa keamanan pada beberapa protokol *IoT* utama:

1. Keamanan MQTT (Message Queuing Telemetry Transport)

   MQTT dirancang sebagai protokol ringan, sehingga tidak memiliki mekanisme keamanan bawaan yang kuat. Namun, ada beberapa cara untuk menambahkan lapisan keamanan dalam MQTT:

   a. TLS/SSL: Untuk mengamankan komunikasi antara klien MQTT dan broker, TLS (Transport *Layer* Security) atau SSL (Secure Sockets *Layer*) dapat

diterapkan. TLS mengenkripsi data dan menyediakan autentikasi antara klien dan broker.

b. Autentikasi: MQTT memungkinkan autentikasi dengan menggunakan kombinasi username dan password. Meskipun sederhana, pendekatan ini dapat diperkuat dengan menerapkan OAuth atau sistem manajemen identitas yang lebih canggih.
c. Autorisasi: MQTT broker seperti Mosquitto mendukung mekanisme kontrol akses berbasis peran (RBAC), di mana setiap klien diberikan izin untuk membaca atau menulis pada topik tertentu.
d. Ancaman:
    - Serangan man-in-the-middle (MITM) jika TLS tidak digunakan.
    - Denial-of-service (DoS) melalui pengiriman pesan yang berlebihan untuk membanjiri broker.

2. Keamanan CoAP (Constrained Application Protocol)

   CoAP menggunakan UDP, yang secara inheren tidak aman dan tidak dapat diandalkan. Untuk mengatasi masalah ini, CoAP menggunakan mekanisme keamanan tambahan:

   a. DTLS (Datagram Transport *Layer* Security): CoAP menggunakan DTLS untuk menyediakan keamanan yang setara dengan TLS tetapi pada jaringan berbasis UDP. DTLS mengenkripsi pesan CoAP dan melindungi dari penyadapan, pemalsuan, dan manipulasi data.
   b. Autentikasi: CoAP mendukung berbagai metode autentikasi, termasuk kunci simetris dan sertifikat berbasis PKI (Public Key Infrastructure). Ini memungkinkan perangkat saling mengidentifikasi sebelum bertukar data.
   c. Integritas Data: DTLS menyediakan integritas data melalui hash-based message authentication codes (HMACs) untuk memastikan pesan tidak dimodifikasi selama transmisi.
   d. Ancaman:

- Replay attack jika tidak ada mekanisme nonce atau timestamp yang memadai.
- Serangan paket palsu karena CoAP menggunakan UDP yang kurang dapat diandalkan daripada TCP.

3. Keamanan HTTP (HyperText Transfer Protocol)
   Meskipun HTTP adalah protokol yang banyak digunakan di *web*, keamanan dalam konteks *IoT* menuntut lapisan tambahan karena HTTP menggunakan TCP yang lebih berat untuk lingkungan *IoT*.
   a. HTTPS (HTTP Secure): HTTPS menggunakan TLS untuk mengenkripsi data yang ditransmisikan antara klien dan *server*. Ini melindungi data dari penyadapan, memastikan integritas, dan memverifikasi identitas *server*.
   b. Autentikasi: HTTP mendukung berbagai metode autentikasi, seperti basic auth, token-based auth (misalnya JWT), dan sertifikat berbasis PKI.
   c. Ancaman:

- Serangan MITM jika tidak menggunakan HTTPS.
- Serangan brute force pada mekanisme autentikasi yang lemah (misalnya, password sederhana).

BAB IV
TEKNOLOGI *NETWORK IOT*

4.1. Konsep Dasar Jaringan *IoT* (*Internet of Things*)

Internet of Things (*IoT*) menghubungkan berbagai perangkat fisik atau "things" yang dilengkapi dengan sensor, perangkat lunak, dan teknologi lainnya untuk bertukar data melalui internet atau jaringan lain. Jaringan *IoT* adalah infrastruktur yang memungkinkan perangkat tersebut berkomunikasi dan berinteraksi secara efisien.

1. Arsitektur *IoT*
    a. Perangkat Endpoint (Node): Ini adalah perangkat di ujung jaringan yang mengumpulkan atau menerima data, seperti sensor, kamera, atau aktuator. Node ini sering kali memiliki daya komputasi terbatas.
    b. Gateway: Berfungsi sebagai penghubung antara perangkat endpoint dan jaringan utama. Gateway membantu mengubah protokol komunikasi dari perangkat endpoint yang umumnya menggunakan protokol ringan seperti MQTT, ke

jaringan yang lebih kompleks seperti internet.

c. *Cloud*: Banyak aplikasi *IoT* memanfaatkan layanan *Cloud* untuk penyimpanan, analisis data, dan pengelolaan perangkat. Data yang dikumpulkan oleh perangkat endpoint diunggah ke *Cloud* untuk diproses lebih lanjut.

d. Aplikasi: Pengguna atau sistem yang berinteraksi dengan data yang dikumpulkan oleh perangkat *IoT*, baik untuk monitoring, pengendalian, atau pengambilan keputusan otomatis.

2. Klasifikasi Teknologi Jaringan *IoT*

   a. Short-Range Networks: Ini termasuk teknologi seperti Wi-Fi, *Bluetooth*, Zigbee, dan Z-Wave yang digunakan untuk menghubungkan perangkat di area terbatas, seperti di dalam gedung atau rumah.

   b. Long-Range Networks: Ini mencakup teknologi seperti LoRaWAN, Sigfox, dan NB-*IoT* yang memungkinkan komunikasi jarak jauh dengan konsumsi daya

rendah. Teknologi ini ideal untuk aplikasi di daerah pedesaan atau kota pintar yang membutuhkan koneksi jarak jauh.

c. Mesh Networks: Beberapa jaringan *IoT*, seperti Zigbee dan Z-Wave, menggunakan *mesh topology* di mana perangkat tidak hanya bertindak sebagai node endpoint, tetapi juga sebagai repeater yang membantu mengirim data melalui perangkat lain.

4.2. Teknologi Jaringan *IoT* Berbasis Koneksi Nirkabel

Teknologi jaringan nirkabel dalam *IoT* memungkinkan perangkat untuk berkomunikasi tanpa memerlukan kabel fisik, sehingga meningkatkan fleksibilitas dan kemudahan instalasi. Teknologi ini sangat penting dalam aplikasi *IoT* karena sering kali perangkat terpasang di lokasi yang sulit dijangkau atau tersebar luas. Berikut adalah beberapa teknologi jaringan *IoT* berbasis koneksi nirkabel yang umum digunakan:

1. Wi-Fi

Wi-Fi adalah teknologi nirkabel yang memungkinkan perangkat terhubung ke jaringan lokal menggunakan gelombang radio. Wi-Fi beroperasi pada frekuensi 2.4 GHz dan 5 GHz.

- Kelebihan: Kecepatan tinggi, dukungan luas, dan mudah diintegrasikan dengan berbagai perangkat dan sistem.
- Kekurangan: Konsumsi daya tinggi, jangkauan terbatas, dan dapat mengalami interferensi dalam lingkungan dengan banyak perangkat.
- Kegunaan dalam *IoT*: Cocok untuk perangkat yang membutuhkan bandwidth tinggi dan dalam lingkungan yang dekat dengan router atau titik akses, seperti perangkat pintar di rumah.

2. *Bluetooth* dan BLE (*Bluetooth Low Energy*)
   Bluetooth adalah teknologi komunikasi nirkabel yang digunakan untuk mentransfer data dalam jarak pendek. BLE adalah versi *Bluetooth* yang dirancang untuk konsumsi daya rendah.

- Kelebihan: Konsumsi daya rendah (terutama untuk BLE), cocok untuk aplikasi dengan jangkauan pendek.
- Kekurangan: Jangkauan terbatas (umumnya hingga 100 meter untuk *Bluetooth* dan lebih sedikit untuk BLE), bandwidth lebih rendah dibandingkan Wi-Fi.
- Kegunaan dalam *IoT*: Ideal untuk perangkat wearable, sensor kesehatan, dan aplikasi yang memerlukan konsumsi daya minimal, seperti perangkat wearable dan sensor lingkungan.

3. Zigbee

   Zigbee adalah protokol komunikasi nirkabel berbasis IEEE 802.15.4 yang dirancang untuk aplikasi *IoT* dengan kebutuhan konsumsi daya rendah dan jangkauan pendek hingga menengah.

   - Kelebihan: Konsumsi daya rendah, kemampuan mesh networking yang memungkinkan jangkauan yang lebih luas dan jangkauan jaringan yang lebih baik.

- Kekurangan: Bandwidth terbatas, kecepatan transfer data lebih rendah dibandingkan Wi-Fi.
- Kegunaan dalam *IoT*: Banyak digunakan dalam automasi rumah, pengendalian pencahayaan, dan aplikasi smart grid karena kemampuannya untuk membuat jaringan mesh yang efisien.

4. Z-Wave

   Z-Wave adalah protokol komunikasi nirkabel untuk automasi rumah dan kontrol perangkat. Ini juga menggunakan teknologi mesh untuk memperluas jangkauan jaringan.

   - Kelebihan: Jangkauan yang baik melalui jaringan mesh, konsumi daya rendah, dan dukungan luas dalam sistem automasi rumah.
   - Kekurangan: Bandwidth dan kecepatan transfer data lebih rendah dibandingkan dengan Wi-Fi dan *Bluetooth*.
   - Kegunaan dalam *IoT*: Digunakan dalam sistem automasi rumah dan pengendalian perangkat rumah pintar seperti kunci pintar, termostat, dan lampu.

4.3. Teknologi Jaringan *IoT* Berbasis Koneksi Jarak Jauh

Teknologi jaringan *IoT* berbasis koneksi jarak jauh memungkinkan perangkat untuk berkomunikasi melalui jarak yang sangat luas, sering kali melintasi wilayah geografis yang besar. Teknologi ini ideal untuk aplikasi *IoT* yang memerlukan cakupan area yang luas atau di lokasi yang terpencil, di mana teknologi nirkabel lokal seperti Wi-Fi atau *Bluetooth* mungkin tidak efektif. Berikut adalah beberapa teknologi jaringan *IoT* berbasis koneksi jarak jauh yang umum digunakan:

1. LoRaWAN (Long Range Wide Area Network)
   LoRaWAN adalah protokol komunikasi nirkabel yang dirancang untuk komunikasi jarak jauh dengan konsumsi daya sangat rendah. Ini beroperasi pada frekuensi sub-GHz, yang memungkinkannya untuk mencapai jangkauan hingga 15 km di daerah terbuka.
   - Kelebihan: Jangkauan yang sangat luas, konsumsi daya rendah, dan biaya operasional yang rendah. Cocok untuk aplikasi dengan perangkat yang tersebar luas.
   - Kekurangan: Bandwidth rendah, kecepatan transfer data terbatas, dan

kapasitas jaringan terbatas pada jumlah perangkat yang dapat berkomunikasi secara bersamaan.

- Kegunaan dalam *IoT*: Ideal untuk aplikasi seperti pemantauan lingkungan, pertanian pintar, dan pengelolaan utilitas, di mana perangkat terdistribusi di area yang luas.

2. NB-*IoT* (Narrowband *IoT*)

   NB-*IoT* adalah teknologi jaringan seluler yang dirancang khusus untuk *IoT*. Ini memberikan jangkauan luas dengan konsumsi daya rendah dan throughput rendah.

   - Kelebihan: Jangkauan luas, penetrasi yang baik di dalam gedung, dan konsumsi daya rendah. Mendukung konektivitas yang andal untuk perangkat *IoT* di area yang sulit dijangkau.
   - Kekurangan: Kecepatan data rendah dibandingkan dengan teknologi seluler lainnya seperti 4G/5G. Keterbatasan dalam kapasitas transfer data per perangkat.

- Kegunaan dalam *IoT*: Digunakan untuk aplikasi seperti pelacakan aset, sensor pintar di kota, dan perangkat dengan kebutuhan data rendah yang tersebar di area luas.

3. Sigfox

   Sigfox adalah teknologi LPWAN (Low Power Wide Area Network) yang menyediakan konektivitas nirkabel dengan jangkauan luas dan konsumsi daya rendah. Ini beroperasi pada frekuensi sub-GHz.

   - Kelebihan: Jangkauan yang sangat luas, biaya operasional rendah, dan konsumsi daya yang sangat rendah. Ideal untuk aplikasi dengan transmisi data yang tidak sering.
   - Kekurangan: Bandwidth rendah dan kapasitas transmisi data per pesan terbatas. Tidak cocok untuk aplikasi yang memerlukan transfer data berukuran besar secara rutin.
   - Kegunaan dalam *IoT*: Cocok untuk pelacakan kendaraan, sensor lingkungan, dan aplikasi kota pintar

yang memerlukan komunikasi jarak jauh dengan kebutuhan data rendah.

4. LTE-M (Long Term Evolution for Machines)
   LTE-M adalah versi LTE (Long Term Evolution) yang dioptimalkan untuk *IoT*. Ini mendukung komunikasi data dengan kecepatan menengah dan konsumsi daya rendah.
   - Kelebihan: Kecepatan data yang lebih baik dibandingkan dengan NB-*IoT*, kemampuan untuk mendukung aplikasi yang memerlukan lebih banyak data, dan cakupan jaringan yang luas.
   - Kekurangan: Konsumsi daya sedikit lebih tinggi dibandingkan dengan teknologi LPWAN seperti LoRaWAN dan Sigfox. Biaya operasional mungkin lebih tinggi.
   - Kegunaan dalam *IoT*: Ideal untuk aplikasi yang memerlukan kecepatan data menengah seperti pelacakan kendaraan, sistem pembayaran, dan aplikasi industri yang memerlukan komunikasi data yang lebih baik.

4.4. Teknologi Jaringan *IoT* Berdasarkan Koneksi Kabel

Teknologi jaringan kabel untuk *IoT* melibatkan penggunaan kabel fisik untuk menghubungkan perangkat dan sistem dalam jaringan *IoT*. Meskipun koneksi nirkabel sering kali lebih fleksibel dan lebih mudah diatur, koneksi kabel masih memiliki keunggulan tertentu dalam hal keandalan, kecepatan, dan keamanan. Berikut adalah beberapa teknologi jaringan kabel yang digunakan dalam *IoT*:

1. Ethernet

   Ethernet adalah teknologi jaringan kabel yang menggunakan kabel twisted pair atau kabel fiber optic untuk menghubungkan perangkat dalam jaringan lokal (LAN). Ethernet adalah salah satu metode koneksi yang paling umum digunakan dalam jaringan komputer.

   - Kelebihan: Kecepatan tinggi, keandalan, latensi rendah, dan keamanan. Ethernet juga mendukung berbagai standar kecepatan dari 10 Mbps hingga 100 Gbps.
   - Kekurangan: Memerlukan instalasi kabel fisik, yang dapat menjadi tidak praktis di beberapa lingkungan atau

untuk aplikasi yang membutuhkan mobilitas tinggi.

- Kegunaan dalam *IoT*: Ideal untuk aplikasi *IoT* di lingkungan yang memerlukan kecepatan tinggi dan keandalan, seperti data center, sistem pemantauan industri, dan infrastruktur jaringan di gedung.

2. Modbus

   Modbus adalah protokol komunikasi yang digunakan untuk menghubungkan perangkat dalam sistem otomasi industri. Ini sering digunakan dalam sistem kontrol berbasis kabel yang menghubungkan perangkat seperti PLC (Programmable Logic Controller) dan sensor.

   - Kelebihan: Sederhana dan dapat diimplementasikan dengan mudah pada jaringan kabel, dan mendukung komunikasi yang handal di lingkungan industri.
   - Kekurangan: Tidak menyediakan enkripsi atau fitur keamanan lanjutan, dan memiliki kecepatan data yang lebih rendah dibandingkan dengan beberapa teknologi kabel modern.

- Kegunaan dalam *IoT*: Banyak digunakan dalam otomasi industri, pengendalian proses, dan sistem pemantauan berbasis sensor di lingkungan industri.

4.5. Tantangan dalam Teknologi Jaringan *IoT*

Teknologi jaringan *IoT* menghadapi berbagai tantangan dalam implementasi dan pengelolaan, terutama seiring dengan pertumbuhan jumlah perangkat dan kompleksitas aplikasi. Berikut adalah beberapa tantangan utama yang dihadapi oleh teknologi jaringan *IoT*:

1. Skalabilitas

   Skalabilitas merujuk pada kemampuan jaringan untuk mengakomodasi jumlah perangkat dan data yang terus berkembang tanpa penurunan kinerja.

   a. Tantangan:

      - Jumlah Perangkat: Dengan bertambahnya perangkat *IoT*, jaringan harus mampu menangani komunikasi antara jutaan perangkat tanpa mengalami kemacetan atau penurunan kinerja.

- Manajemen Jaringan: Mengelola konfigurasi, pemantauan, dan pemeliharaan perangkat dalam jaringan yang sangat besar dapat menjadi rumit dan memerlukan sumber daya yang signifikan.

b. Solusi Potensial:

- Arsitektur Terdistribusi: Menggunakan arsitektur jaringan yang terdistribusi untuk menghindari bottleneck pada titik-titik tertentu.
- Teknologi Virtualisasi: Mengimplementasikan virtualisasi jaringan untuk meningkatkan fleksibilitas dan efisiensi.

2. Efisiensi Energi

Efisiensi energi berkaitan dengan konsumsi daya oleh perangkat *IoT* dan infrastruktur jaringan.

a. Tantangan:

- Daya Perangkat: Banyak perangkat *IoT*, terutama yang berada di lokasi terpencil, harus beroperasi dengan

sumber daya energi terbatas, seperti baterai.

- Pengelolaan Energi: Memerlukan strategi pengelolaan energi yang efektif untuk memperpanjang umur perangkat dan mengurangi frekuensi penggantian baterai.

b. Solusi Potensial:

- Teknologi Low Power: Menggunakan teknologi seperti LPWAN (Low Power Wide Area Network) untuk mengurangi konsumsi daya.
- Optimasi Protokol: Mengoptimalkan protokol komunikasi untuk mengurangi overhead dan konsumsi energi.

3. Keterbatasan Bandwidth

Bandwidth merujuk pada kapasitas saluran komunikasi untuk mentransfer data antara perangkat.

a. Tantangan:

- Kapasitas Jaringan: Banyak perangkat *IoT* mungkin menghasilkan volume data yang

sangat besar, yang dapat membebani kapasitas jaringan dan menyebabkan kemacetan.

- Kualitas Layanan (QoS): Menjamin kualitas layanan yang konsisten untuk berbagai aplikasi dengan kebutuhan bandwidth yang berbeda dapat menjadi tantangan.

b. Solusi Potensial:

- Manajemen Bandwidth: Mengimplementasikan teknik manajemen bandwidth untuk mengatur aliran data dan prioritas.
- Teknologi Kompresi: Menggunakan teknologi kompresi data untuk mengurangi ukuran data yang dikirimkan melalui jaringan.

BAB V
INTEROPERABILITAS IOT

5.1. Konsep Dasar Interoperabilitas *IoT*

Interoperabilitas dalam konteks *Internet of Things* (*IoT*) mengacu pada kemampuan perangkat, sistem, dan aplikasi yang berbeda untuk bekerja sama dan bertukar data secara efektif, meskipun mereka mungkin menggunakan teknologi, standar, atau protokol yang berbeda. Konsep dasar ini sangat penting untuk menciptakan ekosistem *IoT* yang terintegrasi dan berfungsi dengan baik.

1. Definisi Interoperabilitas *IoT*

   Interoperabilitas adalah kemampuan sistem atau perangkat yang berbeda untuk beroperasi bersama, berbagi data, dan bekerja secara sinergis. Dalam *IoT*, ini berarti bahwa perangkat dan aplikasi dari berbagai produsen atau platform dapat saling berkomunikasi dan berfungsi bersama dengan lancar.
2. Klasifikasi Interoperabilitas
   a. Interoperabilitas Teknis: Berkaitan dengan aspek teknis komunikasi dan

integrasi, seperti protokol komunikasi, format data, dan antarmuka.

b. Interoperabilitas Semantik: Berkaitan dengan makna data yang dipertukarkan, sehingga data dari berbagai sumber dapat dipahami dan diinterpretasikan dengan cara yang konsisten.

c. Interoperabilitas Organisasi: Mengacu pada keselarasan proses dan kebijakan antar organisasi atau entitas yang terlibat dalam ekosistem *IoT*.

3. Tantangan Utama

a. Ketidakcocokan Protokol: Berbagai perangkat mungkin menggunakan protokol komunikasi yang berbeda, yang dapat menghambat pertukaran data.

b. Format Data yang Berbeda: Perangkat atau aplikasi mungkin menggunakan format data yang berbeda, membuat integrasi menjadi sulit.

c. Keterbatasan Standar: Kurangnya standar industri yang konsisten dapat menyebabkan kesulitan dalam menciptakan interoperabilitas.

d. Keamanan dan Privasi: Menjaga keamanan dan privasi saat mengintegrasikan berbagai sistem dapat menjadi tantangan besar.

4. Manfaat Interoperabilitas
    a. Efisiensi: Memungkinkan perangkat dan aplikasi untuk bekerja sama dengan lebih efisien, mengurangi kebutuhan untuk integrasi manual.
    b. Skalabilitas: Mempermudah penambahan perangkat dan aplikasi baru ke dalam ekosistem *IoT* yang ada.
    c. Inovasi: Mendorong inovasi dengan memungkinkan berbagai solusi untuk bekerja bersama dan menciptakan nilai baru.

5.2. Model Interoperabilitas dalam *IoT*

Interoperabilitas dalam *IoT* merupakan kunci bagi berbagai perangkat, aplikasi, dan platform untuk bekerja bersama secara efisien, meskipun berasal dari produsen atau menggunakan teknologi yang berbeda. Model interoperabilitas memberikan pendekatan terstruktur untuk memahami dan mengelola bagaimana perangkat-perangkat *IoT* saling berinteraksi. Dua

pendekatan utama yang sering digunakan dalam interoperabilitas *IoT* adalah Model Lapisan dan Model Integrasi.

1. Model Lapisan (*Layer*ed Model)

   Model lapisan untuk interoperabilitas diadopsi dari konsep arsitektur jaringan tradisional, seperti OSI (Open Systems Interconnection) Model atau TCP/IP Model, di mana komunikasi dibagi menjadi beberapa lapisan yang saling mendukung. Setiap lapisan memiliki tugas khusus, dan interoperabilitas dicapai dengan memastikan bahwa lapisan-lapisan ini dapat bekerja bersama dengan baik.

   Komponen Utama dalam Model Lapisan:

   a. Lapisan Perangkat (*Device Layer*): Mencakup perangkat fisik *IoT* seperti sensor, aktuator, dan perangkat yang terhubung ke jaringan. Lapisan ini berfokus pada interoperabilitas perangkat keras.

   b. Lapisan Jaringan (Network *Layer*): Berfokus pada komunikasi data antara perangkat, yang mencakup protokol jaringan seperti IPv6, 6LoWPAN, dan protokol komunikasi seperti MQTT atau

CoAP. Pada lapisan ini, interoperabilitas dicapai dengan memastikan bahwa perangkat dapat bertukar data melalui jaringan yang sama.

c. Lapisan Transportasi (Transport *Layer*): Menjamin pengiriman data yang andal antara perangkat *IoT*. Protokol yang sering digunakan di sini adalah TCP (Transmission Control Protocol) atau UDP (User Datagram Protocol), dan interoperabilitas tercapai dengan standar pengiriman data yang seragam.

d. Lapisan Aplikasi (Application *Layer*): Melibatkan protokol dan standar yang digunakan oleh aplikasi untuk saling berkomunikasi dan berbagi data. Ini bisa mencakup format data seperti JSON atau XML, dan standar komunikasi seperti HTTP, CoAP, atau *Web*Socket.

2. Model Integrasi (Integration Model)

   Model integrasi menekankan bagaimana berbagai komponen dari sistem yang berbeda diintegrasikan menjadi satu sistem yang utuh. Alih-alih membagi sistem menjadi lapisan-lapisan, model ini lebih berfokus pada

penghubungan berbagai elemen melalui platform, middleware, atau teknologi integrasi lain untuk mencapai interoperabilitas.

Komponen Utama dalam Model Integrasi:

a. Middleware: Perangkat lunak yang bertindak sebagai penghubung antara aplikasi, perangkat, atau sistem yang berbeda. Middleware memudahkan komunikasi dan pertukaran data antara perangkat *IoT*, meskipun mereka menggunakan protokol atau format data yang berbeda.
b. API (Application Programming Interface): Digunakan untuk menghubungkan aplikasi yang berbeda dalam ekosistem *IoT*. API memungkinkan perangkat lunak yang berbeda untuk saling bertukar data dan fungsionalitas. API dapat disediakan oleh penyedia platform *IoT* untuk memfasilitasi integrasi antar-platform.
c. Gateway *IoT*: Perangkat yang menjembatani komunikasi antara jaringan *IoT* yang berbeda. Gateway memungkinkan perangkat *IoT* yang

menggunakan protokol komunikasi yang berbeda untuk berkomunikasi satu sama lain melalui proses konversi protokol.

d. Semantic *Web* Technologies: Teknologi semantik seperti RDF (Resource Description Framework) dan OWL (*Web* Ontology Language) digunakan untuk memastikan bahwa data dari perangkat yang berbeda dapat dipahami dan diintegrasikan dengan makna yang konsisten.

5.3. Keamanan dan Privasi dalam Interoperabilitas *IoT*

Keamanan dan privasi merupakan aspek yang sangat penting dalam interoperabilitas *Internet of Things* (*IoT*). Karena ekosistem *IoT* melibatkan berbagai perangkat, protokol, jaringan, dan platform yang berkomunikasi satu sama lain, risiko keamanan yang dihadapi juga menjadi semakin kompleks. Selain itu, karena *IoT* sering melibatkan data pribadi, menjaga privasi pengguna menjadi tantangan besar.

Berikut adalah keamanan dan privasi dalam interoperabilitas *IoT* serta tantangan dan solusi terkait :

1. Tantangan Keamanan dalam Interoperabilitas *IoT*
    a. Kerentanan Jaringan Perangkat *IoT* sering kali terhubung melalui jaringan publik atau jaringan dengan tingkat keamanan yang berbeda-beda. Setiap celah keamanan pada jaringan dapat dimanfaatkan oleh pihak yang tidak berwenang untuk mengakses atau mengontrol perangkat *IoT*. Ketika berbagai perangkat yang terhubung menggunakan standar protokol yang berbeda, mengamankan setiap titik koneksi menjadi lebih sulit.
    b. Autentikasi dan Otorisasi Dalam ekosistem *IoT* yang heterogen, memastikan bahwa setiap perangkat yang terhubung adalah perangkat yang sah (autentikasi) dan memiliki izin untuk melakukan tindakan tertentu (otorisasi) adalah tantangan besar. Banyak perangkat *IoT* tidak memiliki kapasitas untuk menjalankan protokol keamanan yang kompleks, sehingga rentan terhadap serangan seperti spoofing atau man-in-the-middle (MitM).

c. Serangan pada Data Data yang dikirimkan antar perangkat *IoT* dapat diintersepsi atau dimanipulasi jika tidak ada langkah-langkah enkripsi yang tepat. Serangan seperti sniffing dan eavesdropping dapat mengakibatkan pencurian data sensitif, yang dapat berisiko tinggi jika data tersebut menyangkut informasi pribadi atau data industri kritis.

d. Malware dan Botnet Perangkat *IoT* sering kali menjadi target serangan malware atau botnet yang bisa mengontrol ribuan perangkat untuk digunakan dalam serangan DDoS (Distributed Denial of Service). Karena perangkat *IoT* umumnya memiliki kemampuan pemrosesan yang terbatas, banyak dari mereka tidak dilengkapi dengan mekanisme perlindungan yang memadai terhadap serangan ini.

2. Tantangan Privasi dalam Interoperabilitas *IoT*

a. Pengumpulan Data Berlebihan Perangkat *IoT* sering mengumpulkan data dari lingkungan mereka untuk berfungsi. Namun, pengumpulan data yang berlebihan atau tanpa persetujuan pengguna dapat

melanggar privasi. Karena interoperabilitas memungkinkan perangkat dari berbagai platform untuk berkomunikasi, data pribadi pengguna dapat dengan mudah disebarkan atau dibagikan tanpa kontrol yang tepat.

b. Pelacakan dan Pengawasan Perangkat *IoT*, terutama yang terhubung dengan GPS atau sensor lokasi, dapat menimbulkan risiko pelacakan dan pengawasan yang tidak diinginkan. Ketika perangkat dari berbagai produsen saling berinteraksi, informasi lokasi dan perilaku pengguna dapat dikompromikan atau digunakan untuk tujuan yang melanggar privasi.

c. Kepatuhan terhadap Regulasi Privasi Dengan berkembangnya regulasi seperti GDPR (General Data Protection Regulation) di Eropa atau CCPA (California Consumer Privacy Act) di Amerika Serikat, menjaga privasi data menjadi semakin penting. Sistem *IoT* yang saling terhubung dari berbagai negara dan wilayah harus memastikan kepatuhan terhadap regulasi ini. Namun, dengan adanya berbagai sistem

interoperable, menegakkan standar privasi yang konsisten menjadi lebih menantang.

3. Solusi untuk Keamanan dan Privasi dalam Interoperabilitas *IoT*
    a. Enkripsi Data Mengamankan data yang ditransmisikan antara perangkat *IoT* dengan menggunakan enkripsi end-to-end (E2E) sangat penting untuk melindungi data dari intersepsi dan manipulasi. Protokol keamanan seperti TLS (Transport *Layer* Security) dapat digunakan untuk mengenkripsi data yang ditransmisikan di seluruh ekosistem *IoT*.
    b. Autentikasi dan Otorisasi Berlapis Menggunakan metode autentikasi berlapis (multi-factor authentication) dan otorisasi berbasis peran (role-based access control) dapat membantu memastikan bahwa hanya perangkat yang sah yang dapat mengakses sistem dan data tertentu. Protokol seperti OAuth dan X.509 certificates dapat digunakan untuk mengamankan komunikasi antar perangkat.
    c. Keamanan Berbasis Perangkat Solusi keamanan juga harus diterapkan pada level

perangkat, termasuk penggunaan secure boot dan trusted execution environments (TEE) untuk memastikan bahwa perangkat hanya menjalankan perangkat lunak yang sah dan tidak dimanipulasi.

d. Pengelolaan Privasi dengan Desain Prinsip Privacy by Design harus diterapkan dalam pengembangan perangkat dan aplikasi *IoT*. Hal ini mencakup pendekatan untuk meminimalkan pengumpulan data yang tidak diperlukan, memberi kontrol penuh kepada pengguna atas data mereka, serta menggunakan metode anonymization dan pseudonymization untuk melindungi privasi.

e. Middleware Keamanan Middleware yang mendukung keamanan juga dapat diimplementasikan untuk mengelola autentikasi, enkripsi, dan kebijakan akses pada berbagai perangkat *IoT* yang terhubung. Middleware ini dapat memfasilitasi interoperabilitas dengan memastikan bahwa perangkat yang berbeda tetap memenuhi standar keamanan yang diperlukan.

5.4. Implementasi Interoperabilitas *IoT* di Berbagai Industri

1. Sektor Kesehatan

   Interoperabilitas *IoT* dalam sektor kesehatan memungkinkan perangkat dan sistem kesehatan yang berbeda untuk berbagi data secara efektif. Contohnya, perangkat wearable yang memantau detak jantung pasien dapat berkomunikasi dengan sistem rekam medis elektronik (EMR), memungkinkan dokter untuk memantau kondisi pasien secara *real-time*. Hal ini meningkatkan efisiensi dalam perawatan kesehatan dan mengurangi kesalahan. Interoperabilitas juga penting dalam mengintegrasikan berbagai perangkat dari produsen yang berbeda, misalnya monitor tekanan darah, insulin pump, atau perangkat pencitraan medis.

2. Sektor Transportasi

   Dalam sektor transportasi, interoperabilitas *IoT* sangat penting untuk menghubungkan berbagai sistem kendaraan dan infrastruktur transportasi. Contohnya, kendaraan otonom memerlukan kemampuan untuk berkomunikasi dengan sistem lalu lintas cerdas, seperti lampu lalu lintas yang dilengkapi sensor *IoT*. Selain itu,

interoperabilitas memungkinkan sistem pemantauan kendaraan, navigasi, dan pemeliharaan untuk berbagi informasi secara *real-time*, mengoptimalkan rute, mengurangi kemacetan, dan meningkatkan keselamatan di jalan.

3. Smart Cities

   Implementasi *IoT* dalam smart cities bertujuan untuk meningkatkan efisiensi, keberlanjutan, dan kualitas hidup warga kota. Interoperabilitas *IoT* di smart cities memungkinkan berbagai sistem, seperti pengelolaan limbah, pencahayaan jalan, dan jaringan energi, berkomunikasi dan bekerja sama. Misalnya, sensor *IoT* yang dipasang di jalan dapat mengumpulkan data lalu lintas yang kemudian digunakan oleh sistem manajemen transportasi untuk mengatur lampu lalu lintas dan mengurangi kemacetan. Dengan interoperabilitas, semua komponen kota pintar dapat saling berbagi data secara mulus, memungkinkan pengelolaan kota yang lebih cerdas dan efisien.

4. Industri Manufaktur

Dalam industri manufaktur, *IoT* membantu mengotomatisasi proses produksi melalui integrasi mesin-mesin pintar dan sistem manufaktur yang saling terhubung. Interoperabilitas di sini penting untuk memungkinkan mesin-mesin dari berbagai vendor dan teknologi yang berbeda bekerja secara harmonis. Dengan adanya interoperabilitas *IoT*, data produksi dari berbagai tahapan dapat dipantau dan dianalisis secara *real-time*, memungkinkan prediksi kegagalan mesin, peningkatan kualitas produk, dan pengurangan downtime. Contoh lainnya adalah penggunaan *IoT* dalam rantai pasokan, di mana data tentang bahan baku dan produk dapat dilacak dengan akurat untuk memastikan efisiensi.

BAB VI
PLATFORM IOT

6.1. Komponen Utama Platform *IoT*

1. Sensor dan Aktuator

   Sensor dan aktuator adalah elemen fisik utama yang digunakan dalam ekosistem *IoT*.

   - Sensor berfungsi untuk mendeteksi perubahan di lingkungan fisik, seperti suhu, kelembaban, cahaya, tekanan, atau gerakan, dan mengubahnya menjadi data digital yang dapat diolah.
   - Aktuator adalah perangkat yang menerima perintah dari sistem dan menindaklanjutinya dengan menghasilkan aksi fisik, seperti mengaktifkan mesin atau membuka pintu.

2. Perangkat *IoT* (*Edge* Devices)

   Perangkat *IoT* adalah elemen yang mengumpulkan data dari sensor dan berfungsi sebagai penghubung antara dunia fisik dan digital. Contohnya adalah kamera keamanan, perangkat wearable (misalnya, smartwatch), atau termostat pintar. Perangkat ini memiliki

kemampuan untuk memproses data sebelum dikirimkan ke *Cloud* atau pusat data.

3. Konektivitas dan Jaringan

   Komponen konektivitas memungkinkan perangkat *IoT* untuk terhubung dengan platform *Cloud* atau *server*, tempat data disimpan dan dianalisis. Ada berbagai jenis koneksi yang digunakan, tergantung pada kebutuhan daya, jangkauan, dan kecepatan, seperti:

   - Wi-Fi: Umum digunakan untuk aplikasi *IoT* di rumah atau kantor.
   - *Bluetooth*: Digunakan dalam aplikasi jarak dekat seperti wearable atau perangkat kesehatan.
   - LoRa dan Zigbee: Protokol jaringan yang lebih hemat energi dan dapat digunakan untuk perangkat dengan daya rendah, terutama di area yang luas seperti pertanian atau industri.

4. Platform *Cloud* untuk *IoT*

   Platform *Cloud IoT* adalah pusat pengelolaan data. Ini menyediakan kapasitas penyimpanan yang luas dan kemampuan untuk memproses data secara *real-time*. Platform *Cloud* seperti

AWS *IoT*, Microsoft Azure *IoT*, atau Google *Cloud IoT* mendukung pemrosesan, pengelolaan perangkat, dan penyajian data secara efisien.

5. Antarmuka Pengguna (UI/UX)

   Antarmuka pengguna adalah bagian yang memungkinkan manusia berinteraksi dengan sistem *IoT*. Misalnya, aplikasi ponsel yang mengontrol perangkat rumah pintar atau dashboard untuk mengelola data yang dihasilkan dari jaringan sensor *IoT*. Desain UI/UX harus responsif, mudah digunakan, dan menyajikan informasi dengan cara yang mudah dipahami.

6.2. Arsitektur Platform *IoT*

Arsitektur Platform *IoT* terdiri dari beberapa lapisan (*Layer*s) yang bekerja secara sinergis untuk memungkinkan perangkat, sensor, dan aplikasi *IoT* berfungsi secara efisien. Berikut adalah lapisan-lapisan utama dalam arsitektur platform *IoT*:

1. *Layer* Perangkat Fisik (Perception *Layer*)

   Lapisan ini mencakup sensor, aktuator, dan perangkat *IoT* yang menangkap data dari lingkungan fisik.

- Sensor: Mendeteksi berbagai parameter lingkungan seperti suhu, kelembaban, cahaya, dan lainnya.
- Aktuator: Menerima perintah dari platform *IoT* dan menghasilkan aksi fisik seperti menggerakkan motor atau membuka katup.
- Perangkat *IoT*: Ini bisa berupa perangkat sederhana atau kompleks seperti kamera keamanan, termostat pintar, atau perangkat wearable.

2. *Layer* Konektivitas (Network *Layer*)

   Lapisan konektivitas bertanggung jawab untuk menghubungkan perangkat *IoT* ke platform *Cloud* atau data center melalui jaringan. Protokol yang digunakan tergantung pada kebutuhan bandwidth, latensi, dan jangkauan, seperti:

   - Wi-Fi: Digunakan untuk area cakupan yang lebih kecil seperti rumah atau kantor.
   - 4G/5G: Mendukung komunikasi *IoT* di area yang lebih luas dengan kecepatan tinggi.

- Protokol *IoT* seperti Zigbee, LoRa, dan NB-*IoT*: Dirancang khusus untuk komunikasi jarak jauh dengan konsumsi daya rendah, cocok untuk aplikasi seperti pertanian atau industri besar.

3. *Layer* Data dan Analisis (Data Processing *Layer*)
   Setelah data ditangkap oleh perangkat dan dikirim melalui jaringan, lapisan ini memproses dan menganalisis data secara *real-time*. Di sinilah pemrosesan data terjadi, baik secara lokal (*edge computing*) atau di *Cloud*. Fungsi utama *Layer* ini adalah:
   - Pemrosesan Data: Menganalisis data yang masuk untuk menghasilkan wawasan berharga, seperti pola penggunaan energi atau deteksi anomali.
   - Storage (Penyimpanan Data): Menyimpan data yang dihasilkan untuk keperluan historis dan analisis lebih lanjut.
   - *Big data* Analytics: Teknologi *big data* sering digunakan untuk memproses dan menganalisis sejumlah besar data *IoT*

untuk mengambil keputusan berbasis data.

4. *Layer* Aplikasi (Application *Layer*)

   Lapisan ini adalah antarmuka antara pengguna dan platform *IoT*, di mana aplikasi dibangun berdasarkan data yang dikumpulkan. Beberapa aplikasi *IoT* di berbagai sektor meliputi:

   - Smart Home: Sistem otomatisasi rumah yang memungkinkan pengelolaan perangkat rumah tangga jarak jauh.
   - Smart City: Sistem yang mengelola infrastruktur kota seperti lampu jalan, lalu lintas, dan sistem air.
   - Industrial *IoT* (I*IoT*): Digunakan untuk pemeliharaan prediktif dan optimasi produksi di industri manufaktur.

5. *Layer* Keamanan (Security *Layer*)

   Keamanan merupakan aspek penting dalam *IoT* karena banyaknya data yang dihasilkan dan dikirim antar perangkat. Lapisan ini melibatkan:

   - Enkripsi Data: Untuk menjaga privasi dan kerahasiaan data yang dikirim.
   - Otentikasi dan Pengelolaan Identitas: Untuk memastikan bahwa hanya

perangkat yang sah yang dapat terhubung ke platform.

- Pengamanan Jaringan: Mengamankan jaringan dari serangan seperti Distributed Denial of Service (DDoS).

6. *Layer* Pengelolaan (Management *Layer*)

   Lapisan ini bertanggung jawab untuk mengelola perangkat *IoT* yang terhubung. Fungsi ini meliputi:

   - Pengelolaan Perangkat: Mengontrol, memantau, dan memperbarui perangkat *IoT* secara jarak jauh.
   - Pengelolaan Konfigurasi: Mengatur konfigurasi perangkat dan memastikan semua perangkat berfungsi sesuai parameter yang telah ditentukan.

6.3. Fungsi Utama Platform *IoT*

Platform *Internet of Things* (*IoT*) memainkan peran penting dalam mengelola dan mengoptimalkan interaksi antara perangkat pintar, sensor, jaringan, dan aplikasi. Berikut adalah fungsi utama dari platform *IoT*:

1. Pengelolaan Perangkat (Device Management)

Platform *IoT* berfungsi untuk mengelola perangkat yang terhubung di seluruh jaringan. Ini mencakup berbagai aspek, termasuk:

- Pendaftaran dan Otentikasi Perangkat: Platform *IoT* mengatur proses menambahkan perangkat baru ke dalam jaringan, memastikan setiap perangkat yang terhubung telah d*IoT*orisasi.
- Monitoring: Platform memungkinkan pengelolaan status dan kesehatan perangkat secara *real-time*, seperti memantau kondisi baterai atau memastikan perangkat berfungsi dengan baik.
- Pembaruan Firmware Jarak Jauh: Platform *IoT* juga mendukung pembaruan software secara jarak jauh, memungkinkan pemeliharaan perangkat secara efisien.

2. Pemrosesan Data dan Analitik

   Salah satu fungsi utama platform *IoT* adalah mengumpulkan, memproses, dan menganalisis data yang dihasilkan oleh perangkat *IoT*.

3. Keamanan dan Enkripsi Data

Keamanan adalah prioritas utama dalam *IoT* karena banyaknya data sensitif yang dikirimkan antar perangkat dan platform.

4. Integrasi dengan Sistem Lain

   Platform *IoT* sering kali diintegrasikan dengan sistem perangkat lunak lainnya, seperti Enterprise Resource Planning (ERP) atau Customer Relationship Management (CRM), untuk memperkaya data dan fungsionalitas yang dimiliki oleh organisasi.

5. Automasi dan Pengendalian Jarak Jauh

   Platform *IoT* mendukung automasi proses serta pengendalian perangkat jarak jauh.

6. Manajemen Perangkat Lunak (Software Management)

   Platform *IoT* memungkinkan pengelolaan aplikasi dan perangkat lunak yang terpasang di perangkat *IoT*.

7. Kompatibilitas Multi-Vendor

   Platform *IoT* yang baik memungkinkan integrasi perangkat dari berbagai vendor dan memastikan bahwa perangkat dari produsen yang berbeda dapat bekerja sama dengan baik dalam ekosistem yang sama. Ini menghindari

ketergantungan pada satu vendor dan memungkinkan fleksibilitas yang lebih besar.

6.4. Jenis-Jenis *Platform IoT*

Platform *IoT* (*Internet of Things*) hadir dalam berbagai jenis berdasarkan tujuan, penggunaan, dan arsitekturnya. Pemilihan jenis platform *IoT* tergantung pada kebutuhan spesifik industri, perangkat, dan jenis data yang dikelola. Berikut adalah beberapa jenis utama dari platform *IoT*:

1. Platform *IoT* Terbuka (Open Source) vs. Proprietary
    - Platform *IoT* Terbuka (Open Source): Platform ini menawarkan akses terbuka ke kode sumbernya, memungkinkan pengguna untuk memodifikasi, mengadaptasi, dan menyesuaikan platform sesuai dengan kebutuhan spesifik mereka. Contoh platform terbuka termasuk ThingsBoard dan Kaa *IoT*. Keuntungan utamanya adalah fleksibilitas tinggi dan biaya yang lebih rendah, tetapi memerlukan pengetahuan teknis yang lebih dalam.
    - Platform *IoT* Proprietary: Platform ini dikembangkan oleh perusahaan atau vendor

tertentu dan biasanya memiliki fitur, keamanan, dan dukungan teknis yang kuat. Contoh platform proprietary meliputi Amazon *Web* Services (AWS) *IoT*, Microsoft Azure *IoT*, dan Google *Cloud IoT*. Mereka menawarkan solusi yang lebih komprehensif dengan layanan terintegrasi, namun biaya dan ketergantungan pada vendor bisa lebih tinggi.

2. Platform *IoT* Umum vs. Spesifik Industri
    - Platform *IoT* Umum (General-Purpose *IoT* Platforms): Platform ini dirancang untuk berbagai aplikasi dan tidak terbatas pada industri tertentu. Mereka menyediakan solusi yang dapat digunakan di berbagai sektor, seperti rumah pintar, kota pintar, dan kendaraan terhubung. Contoh platform umum adalah Google *Cloud IoT* dan IBM Watson *IoT*.
    - Platform *IoT* Spesifik Industri (Industry-Specific *IoT* Platforms): Dirancang untuk aplikasi spesifik di sektor industri tertentu, seperti manufaktur, kesehatan, transportasi, atau pertanian. Misalnya, Siemens MindSphere dan PTC ThingWorx fokus pada

aplikasi industri (Industrial *IoT* atau I*IoT*). Platform ini biasanya menawarkan fitur yang lebih sesuai dengan kebutuhan industri, seperti pemeliharaan prediktif dan analisis kinerja mesin.

3. Platform *IoT* untuk Konsumen vs. Industrial *IoT* (I*IoT*)
    - Platform *IoT* untuk Konsumen (Consumer *IoT* Platforms): Digunakan untuk menghubungkan perangkat konsumen seperti perangkat rumah pintar (smart home), wearable (perangkat yang dapat dipakai), dan kendaraan terhubung. Contoh aplikasi mencakup pengelolaan perangkat rumah, seperti Amazon Alexa atau Google Home, yang terintegrasi dengan platform *IoT* untuk mengelola berbagai perangkat.
    - Industrial *IoT* (I*IoT*) Platforms: Fokus pada solusi *IoT* untuk sektor industri dan pabrik. I*IoT* mencakup pemantauan mesin, manajemen energi, dan otomatisasi proses industri. Platform I*IoT* seperti GE Predix dan Siemens MindSphere mendukung efisiensi operasional dan pengelolaan aset industri secara lebih baik.

4. Platform *IoT Cloud* vs. *Edge*
    - *Cloud IoT* Platforms: Mengandalkan *Cloud computing* untuk menyimpan, memproses, dan menganalisis data *IoT*. Platform seperti AWS *IoT* dan Microsoft Azure *IoT* Hub adalah contoh platform berbasis *Cloud* yang menyediakan skalabilitas tinggi, kemampuan analitik data, dan integrasi dengan layanan *Cloud* lainnya. Keuntungan utama dari platform ini adalah kemampuannya untuk menangani data dalam jumlah besar dengan kecepatan tinggi dan integrasi yang mudah.
    - *Edge IoT* Platforms: Menggunakan *edge computing* untuk memproses data lebih dekat ke sumber data (perangkat atau sensor), mengurangi latensi dan bandwidth yang diperlukan untuk mengirim data ke *Cloud*. Platform *IoT* berbasis *edge* seperti *Edge*X Foundry memungkinkan pemrosesan data lokal untuk aplikasi *real-time* dan mengurangi ketergantungan pada *Cloud*. Solusi ini ideal untuk lingkungan yang memerlukan waktu respons cepat dan keterbatasan jaringan.

5. Platform *IoT* Private vs. Public
    - Platform *IoT* Private: Dirancang untuk digunakan dalam lingkungan tertutup atau organisasi tertentu, sering kali di-hosting secara lokal atau dalam infrastruktur *Cloud* pribadi. Platform *IoT* privat menawarkan kontrol penuh atas data dan perangkat, serta keamanan yang lebih tinggi. Contohnya termasuk Cisco *IoT* Control Center yang dirancang untuk penyedia layanan komunikasi.
    - Platform *IoT* Public: Platform ini di-hosting oleh penyedia layanan *Cloud* publik dan biasanya bersifat multitenant (digunakan oleh banyak organisasi), seperti AWS *IoT* Core dan Google *Cloud IoT* Core. Keuntungan dari platform publik adalah skalabilitas dan kemudahan penggunaan, namun mungkin ada risiko privasi dan keamanan yang lebih tinggi.
6. Platform *IoT* Data-Driven vs. Action-Driven
    - Data-Driven Platforms: Platform ini fokus pada pengumpulan, penyimpanan, dan analisis data yang dihasilkan oleh perangkat *IoT*. Mereka mendukung aplikasi analitik

data besar (*big data*) dan pembelajaran mesin (machine learning) untuk memprediksi perilaku atau tren. Contohnya adalah IBM Watson *IoT* yang menawarkan solusi untuk analitik dan kecerdasan buatan (AI) berbasis data *IoT*.

- Action-Driven Platforms: Platform ini dirancang untuk menjalankan tindakan otomatis berdasarkan data yang dikumpulkan, seperti pemeliharaan otomatis atau pengendalian perangkat. Misalnya, Google *Cloud IoT* dapat diintegrasikan dengan Google Assistant untuk memungkinkan automasi rumah pintar yang didorong oleh perintah suara.

BAB VII
FUNDAMENTAL *CLOUD*

7.1. Definisi *Cloud Computing*

Cloud computing adalah model komputasi yang memungkinkan akses on-demand ke sumber daya komputasi seperti *server*, penyimpanan, jaringan, dan aplikasi melalui internet, tanpa perlu pengelolaan langsung dari pengguna. Teknologi ini memungkinkan pengguna untuk menggunakan infrastruktur komputasi secara fleksibel dan efisien, dengan model pembayaran berbasis penggunaan, sehingga mengurangi kebutuhan investasi pada perangkat keras dan perangkat lunak secara lokal.

7.2. Model Layanan *Cloud Computing*

Cloud computing menawarkan tiga model layanan utama, yang masing-masing menyediakan tingkat kontrol, fleksibilitas, dan tanggung jawab yang berbeda. Ketiga model layanan ini adalah Infrastructure as a Service (IaaS), Platform as a Service (PaaS), dan Software as a Service (SaaS).

1. Infrastructure as a Service (IaaS)

IaaS adalah model layanan *Cloud* yang menyediakan infrastruktur TI, termasuk *server* virtual atau fisik, penyimpanan, jaringan, dan komponen perangkat keras lainnya. Pengguna dapat mengelola sistem operasi, aplikasi, dan basis data di infrastruktur ini, tetapi tidak perlu mengelola perangkat keras fisik yang mendasarinya.

- Fungsi utama: Pengguna memiliki kontrol penuh terhadap infrastruktur komputasi dan dapat mengonfigurasi sistem sesuai kebutuhan.
- Contoh penggunaan: Ideal untuk organisasi yang membutuhkan skalabilitas tinggi, seperti hosting situs *web*, database, atau aplikasi perusahaan.
- Contoh layanan IaaS: Amazon *Web* Services (AWS), Microsoft Azure, Google Compute Engine.

2. Platform as a Service (PaaS)

   PaaS menyediakan platform yang memungkinkan pengembang membangun, menguji, dan mengelola aplikasi tanpa harus mengurus infrastruktur dasar seperti *server* atau penyimpanan. Dengan PaaS, pengguna

dapat fokus pada pengembangan aplikasi sementara penyedia layanan *Cloud* mengelola infrastruktur dan sistem operasi.

- Fungsi utama: Menyediakan lingkungan pengembangan siap pakai yang mencakup sistem operasi, database, dan alat pengembangan.
- Contoh penggunaan: Pengembangan aplikasi *web* dan mobile, API, layanan backend.
- Contoh layanan PaaS: Google App Engine, Microsoft Azure App Services, Heroku.

3. Software as a Service (SaaS)

   SaaS adalah model layanan di mana aplikasi perangkat lunak disediakan melalui internet dan diakses langsung oleh pengguna melalui browser *web*. Pengguna tidak perlu mengelola aplikasi atau infrastruktur pendukungnya karena semuanya diatur oleh penyedia *Cloud*.

   - Fungsi utama: Pengguna cukup menggunakan aplikasi tanpa harus melakukan instalasi atau pemeliharaan.
   - Contoh penggunaan: Layanan email, CRM (Customer Relationship Management), ERP (Enterprise Resource Planning).

- Contoh layanan SaaS: Google Workspace, Microsoft Office 365, Salesforce.

Ketiga model layanan ini menawarkan fleksibilitas dan efisiensi dalam pengelolaan teknologi informasi, dan masing-masing memiliki kelebihan serta penggunaannya tergantung pada kebutuhan spesifik organisasi atau individu.

7.3. Model Penyebaran *Cloud Computing*

Model penyebaran *Cloud computing* menentukan bagaimana infrastruktur *Cloud* dikelola dan diakses oleh pengguna. Ada empat model penyebaran utama dalam *Cloud computing*: Public *Cloud*, Private *Cloud*, Hybrid *Cloud*, dan *Community Cloud*. Masing-masing model memiliki karakteristik, kelebihan, dan kekurangan yang berbeda, dan pemilihannya tergantung pada kebutuhan spesifik organisasi atau aplikasi.

1. Public *Cloud*

   Public *Cloud* adalah model di mana layanan *Cloud* disediakan oleh penyedia pihak ketiga dan diakses oleh publik melalui internet. Penyedia *Cloud* bertanggung jawab penuh untuk

manajemen dan pemeliharaan infrastruktur, termasuk *server*, penyimpanan, dan jaringan.

- Kelebihan: Biaya awal rendah, skalabilitas tinggi, dan tidak perlu investasi dalam infrastruktur fisik. Ideal untuk aplikasi dengan kebutuhan sumber daya yang variatif.
- Kekurangan: Kurang kontrol atas keamanan dan privasi data karena sumber daya dibagikan dengan banyak pengguna lain.
- Contoh: Amazon *Web* Services (AWS), Microsoft Azure, Google *Cloud* Platform (GCP).

2. Private *Cloud*

   Private *Cloud* adalah model di mana infrastruktur *Cloud* digunakan secara eksklusif oleh satu organisasi. Private *Cloud* dapat di-host secara on-premises (di dalam fasilitas organisasi) atau oleh penyedia pihak ketiga tetapi dikelola secara privat.

   - Kelebihan: Kontrol penuh atas infrastruktur dan keamanan, dapat disesuaikan dengan kebutuhan spesifik organisasi. Cocok untuk organisasi dengan persyaratan privasi dan kepatuhan yang ketat.

- Kekurangan: Biaya lebih tinggi dan memerlukan investasi awal yang signifikan. Skalabilitas mungkin terbatas dibandingkan dengan public *Cloud*.
- Contoh: VMware *Cloud* Foundation, Microsoft Azure Stack, IBM *Cloud* Private.

3. Hybrid *Cloud*

   Hybrid *Cloud* menggabungkan elemen dari public dan private *Cloud*, memungkinkan data dan aplikasi untuk dipindahkan antara keduanya. Model ini memberikan fleksibilitas dan opsi untuk memanfaatkan sumber daya dari kedua jenis *Cloud*.

   - Kelebihan: Memungkinkan organisasi untuk memanfaatkan kelebihan public *Cloud* untuk beban kerja yang dapat dipublikasikan, sementara tetap menjaga data sensitif di private *Cloud*.
   - Kekurangan: Kompleksitas dalam pengelolaan dan integrasi. Memerlukan strategi yang matang untuk mengelola data dan aplikasi di kedua lingkungan.
   - Contoh: Integrasi antara AWS dan VMware *Cloud* on AWS, Microsoft Azure dengan on-premises data centers.

4. *Community Cloud*

   Community Cloud adalah model di mana infrastruktur *Cloud* digunakan oleh sekelompok organisasi dengan kesamaan kepentingan atau kebutuhan, seperti regulasi atau keamanan. *Cloud* ini dapat dikelola oleh salah satu organisasi atau oleh penyedia pihak ketiga.

   - Kelebihan: Biaya dapat dibagi di antara organisasi yang berbagi *Cloud*, serta peningkatan keamanan dan kepatuhan yang sesuai dengan kebutuhan komunitas tersebut.
   - Kekurangan: Kurang fleksibel dibandingkan dengan public *Cloud* dan mungkin tidak memenuhi kebutuhan unik masing-masing organisasi dalam komunitas.
   - Contoh: *Cloud* untuk lembaga pemerintah, institusi pendidikan, atau organisasi nirlaba yang berbagi sumber daya.

7.4. Kinerja dan Skalabilitas *Cloud Computing*

Kinerja dan skalabilitas adalah dua aspek kunci dalam *Cloud computing* yang memengaruhi bagaimana layanan *Cloud* beroperasi dan memenuhi kebutuhan pengguna.

1. Kinerja *Cloud Computing*

   Kinerja *Cloud computing* mengacu pada seberapa efisien dan cepat layanan *Cloud* dapat memenuhi kebutuhan pengguna, termasuk kecepatan pemrosesan, waktu respons, dan throughput. Faktor-faktor yang mempengaruhi kinerja *Cloud* termasuk:

   a. Latensi: Waktu yang dibutuhkan untuk data melakukan perjalanan dari sumber ke tujuan. Latensi rendah sangat penting untuk aplikasi yang memerlukan respon cepat, seperti aplikasi *real-time* atau streaming.
   b. Throughput: Jumlah data yang dapat diproses atau ditransfer dalam periode waktu tertentu. Throughput tinggi mendukung aplikasi dengan kebutuhan data besar, seperti pemrosesan *big data* atau video streaming.
   c. Ketersediaan: Kemampuan layanan untuk tetap tersedia dan berfungsi tanpa gangguan. Ketersediaan tinggi memastikan bahwa aplikasi tetap dapat diakses meskipun terjadi kegagalan perangkat keras atau jaringan.

d. Keandalan: Seberapa konsisten layanan *Cloud* dalam memberikan performa yang dijanjikan. Keandalan mengurangi risiko kegagalan sistem dan downtime yang tidak terduga.

2. Skalabilitas *Cloud Computing*

   Skalabilitas *Cloud computing* mengacu pada kemampuan sistem untuk menangani peningkatan beban kerja atau jumlah pengguna dengan menambah atau mengurangi sumber daya sesuai kebutuhan. Ada dua jenis utama skalabilitas:

   a. Skalabilitas Vertikal: Meningkatkan kapasitas sistem dengan menambah sumber daya pada *server* tunggal, seperti CPU, RAM, atau penyimpanan. Meskipun ini dapat meningkatkan kinerja, ada batasan fisik pada seberapa banyak sumber daya yang dapat ditambahkan ke satu *server*.

   b. Skalabilitas Horisontal: Meningkatkan kapasitas sistem dengan menambah jumlah *server* atau instansi. Ini memungkinkan sistem untuk menangani beban kerja yang lebih besar dengan membagi beban di antara banyak *server*. Skalabilitas horisontal

sering kali lebih fleksibel dan dapat mengakomodasi pertumbuhan yang lebih besar.

Auto-scaling adalah fitur penting dalam *Cloud computing* yang memungkinkan sistem untuk secara otomatis menyesuaikan jumlah sumber daya yang digunakan berdasarkan permintaan. Misalnya, jika beban kerja meningkat, sistem dapat menambahkan lebih banyak instance *server* untuk menangani permintaan tambahan.

7.5. Manajemen dan Pengelolaan *Cloud*

Manajemen dan pengelolaan *Cloud computing* adalah proses yang melibatkan pemantauan, pengendalian, dan perawatan infrastruktur *Cloud* untuk memastikan operasional yang efisien, aman, dan sesuai dengan kebutuhan organisasi. Ini mencakup berbagai aspek mulai dari pengelolaan sumber daya hingga keamanan dan kepatuhan.

1. Pengelolaan Sumber Daya

   Pengelolaan sumber daya *Cloud* melibatkan alokasi, pemantauan, dan optimisasi sumber daya komputasi, penyimpanan, dan jaringan. Hal ini mencakup:

a. Provisioning dan Konfigurasi: Menyediakan dan mengonfigurasi sumber daya *Cloud* sesuai kebutuhan aplikasi dan beban kerja.
b. Pemantauan dan Penyesuaian: Memantau penggunaan sumber daya secara *real-time* dan menyesuaikan kapasitas sesuai permintaan. Ini sering dilakukan dengan bantuan alat pemantauan dan analisis yang memberikan wawasan tentang performa dan penggunaan.
c. Optimasi Biaya: Mengelola dan mengoptimalkan biaya *Cloud* dengan memilih tipe instansi yang tepat, mengelola penyimpanan secara efisien, dan memanfaatkan model pembayaran berbasis penggunaan untuk mengurangi biaya.

2. Keamanan dan Kepatuhan

   Keamanan dan kepatuhan adalah aspek krusial dalam manajemen *Cloud*. Ini melibatkan:

   a. Kontrol Akses dan Identitas: Mengelola hak akses dan identitas pengguna dengan menggunakan mekanisme seperti Identity and Access Management (IAM) untuk memastikan hanya pengguna yang

berwenang yang dapat mengakses data dan aplikasi.

b. Enkripsi dan Perlindungan Data: Menggunakan enkripsi untuk melindungi data baik saat transit maupun saat disimpan. Ini juga mencakup perlindungan dari ancaman dan serangan siber.

c. Kepatuhan: Memastikan bahwa penggunaan layanan *Cloud* mematuhi standar industri dan regulasi yang relevan, seperti GDPR, HIPAA, atau PCI-DSS.

3. Pengelolaan Layanan *Cloud*

Pengelolaan layanan *Cloud* melibatkan pengaturan dan pemeliharaan aplikasi dan layanan yang berjalan di *Cloud*. Ini termasuk:

a. Manajemen Aplikasi: Melakukan deploy, konfigurasi, dan pembaruan aplikasi *Cloud*. Ini juga mencakup pengelolaan siklus hidup aplikasi dan pemantauan performanya.

b. Backup dan Pemulihan: Menyediakan strategi cadangan dan pemulihan bencana untuk memastikan data dapat dipulihkan jika terjadi kegagalan atau kehilangan data.

c. Automasi dan Orkestrasi: Menggunakan alat otomasi untuk mengelola dan

menyederhanakan proses operasional, serta orkestrasi untuk mengelola dan mengoordinasikan layanan *Cloud* secara efisien.

BAB VIII
SENSOR *CLOUD*

8.1. Pengantar Sensor *Cloud*

8.1.1. Definisi Sensor *Cloud*

Sensor dalam *Internet of Things* (*IoT*) dapat diartikan perangkat yang mampu mendeteksi, mengukur, dan mengumpulkan data dari lingkungan fisik atau objek, lalu mentransmisikan informasi tersebut ke jaringan *IoT* untuk analisis lebih lanjut (Andaria, 2024). Sensor *Cloud* adalah integrasi antara teknologi sensor yang digunakan untuk pengumpulan data dan *Cloud computing* untuk menyimpan, mengolah, dan menganalisis data tersebut. Sensor *Cloud* memungkinkan pengumpulan data sensor secara *real-time* dari berbagai sumber dan kemudian mengirimkannya ke *Cloud* untuk disimpan, diproses, dan dibagikan kepada pengguna yang berbeda. Dalam arsitektur Sensor *Cloud*, sensor bertindak sebagai sumber data yang mengirimkan informasi ke *Cloud* melalui jaringan *IoT*. Menurut publikasi oleh (Gubbi et al., 2013), Sensor *Cloud* menjadi komponen penting dalam *IoT* karena mendukung pengolahan data

dalam jumlah besar dari sensor yang tersebar secara geografis. *Cloud computing* menyediakan fleksibilitas dalam mengelola data secara terdistribusi dan memastikan bahwa pengguna dapat mengakses informasi ini kapan saja melalui internet.

8.1.2. Peran dan Signifikansi dalam *IoT*

Peran Sensor *Cloud* dalam *IoT* sangat penting untuk mendukung ekosistem yang memungkinkan koneksi perangkat-perangkat pintar. Sensor *Cloud* memberikan infrastruktur yang diperlukan untuk mengumpulkan, memproses, dan menganalisis data sensor secara terpusat, sehingga meningkatkan efisiensi dan efektivitas pengelolaan data *IoT*.

Beberapa peran utama Sensor *Cloud* dalam *IoT* meliputi:

1. Pengumpulan Data *Real-time*: Dengan bantuan jaringan sensor, Sensor *Cloud* memungkinkan pengumpulan data dari lingkungan fisik secara *real-time*. Data ini kemudian dikirim ke *Cloud* untuk diproses lebih lanjut.

2. Pengolahan Data: Sensor *Cloud* mengintegrasikan data dari berbagai sensor di lokasi yang berbeda dan melakukan pengolahan berbasis *Cloud*, termasuk analisis data besar (*big data*) untuk menghasilkan informasi yang lebih bermakna.
3. Penyimpanan dan Keamanan Data: Data yang dikumpulkan oleh sensor dapat disimpan di *Cloud* dengan skala yang sangat besar. *Cloud* juga menyediakan lapisan keamanan tambahan untuk melindungi data yang sensitif.
4. Aksesibilitas dan Skalabilitas: Sensor *Cloud* menawarkan fleksibilitas kepada pengguna untuk mengakses data sensor kapan saja dan dari mana saja, serta mudah disesuaikan dengan perubahan jumlah sensor atau data yang dihasilkan.

Menurut (Mollah et al., 2017), Sensor *Cloud* menjadi solusi penting untuk meningkatkan efisiensi sistem *IoT*, terutama dalam hal pengelolaan data dan fleksibilitas pengaksesan informasi dari berbagai perangkat .

8.1.3. Manfaat dan Tantangan Implementasi Sensor *Cloud*

Manfaat Sensor *Cloud* dalam *IoT* mencakup:

1. Pengelolaan Data yang Efisien: *Cloud computing* memungkinkan penanganan volume data yang besar dari sensor, termasuk pemrosesan, penyimpanan, dan analisis yang terpusat.
2. Pemanfaatan Optimal Sumber Daya: Dengan memanfaatkan infrastruktur *Cloud*, biaya operasional dapat ditekan karena tidak diperlukan perangkat keras lokal untuk menyimpan dan memproses data.
3. Peningkatan Skalabilitas: Sensor *Cloud* dapat dengan mudah diperluas sesuai dengan peningkatan jumlah sensor atau volume data.
4. Akses *Real-time*: Data sensor yang disimpan di *Cloud* dapat diakses secara *real-time*, yang penting untuk aplikasi-aplikasi yang membutuhkan respons cepat seperti sistem pemantauan bencana atau transportasi cerdas.

Tantangan Implementasi Sensor *Cloud*:

1. Keamanan dan Privasi Data: Dengan banyaknya data sensor yang bersifat sensitif (misalnya, data kesehatan atau lokasi), memastikan keamanan dan privasi data merupakan tantangan besar.
2. Latency: Pengiriman data ke *Cloud* dan pengolahan di *Cloud* bisa memerlukan waktu tambahan, terutama untuk aplikasi yang membutuhkan respons sangat cepat.
3. Reliabilitas Jaringan: Sensor *Cloud* sangat tergantung pada kualitas koneksi jaringan. Gangguan pada jaringan dapat menyebabkan kehilangan data atau kegagalan dalam pemrosesan *real-time*.
4. Interoperabilitas: Dengan berbagai sensor yang berasal dari produsen yang berbeda, memastikan kompatibilitas dan interoperabilitas antar-perangkat dan layanan *Cloud* menjadi tantangan besar.

Salah satu tantangan terbesar dalam implementasi Sensor *Cloud* adalah memastikan keandalan jaringan dan keamanan data yang tersimpan di *Cloud* (Chen et al., 2014).

8.2. Arsitektur Sensor *Cloud*

Arsitektur Sensor *Cloud* terdiri dari beberapa komponen penting yang bekerja bersama-sama untuk menghubungkan sensor fisik ke platform *Cloud*, memproses data yang dikumpulkan, dan menyediakan layanan untuk berbagai aplikasi berbasis *IoT*. Arsitektur ini dirancang agar memungkinkan pengolahan data yang efisien dan integrasi antara perangkat yang berbeda, jaringan komunikasi, dan platform *Cloud*.

8.2.1. Komponen Utama dalam Arsitektur Sensor *Cloud*

1. Sensor: komponen ini berfungsi sebagai perangkat yang mendeteksi perubahan atau variasi di lingkungan fisik, seperti suhu, tekanan, cahaya, atau gerakan. Sensor ini bertindak sebagai sumber data dalam arsitektur Sensor *Cloud*. Mereka menangkap informasi dari lingkungan mereka dan mengirimkan data tersebut melalui gateway ke *Cloud* untuk diproses lebih lanjut. Sensor dalam *IoT* memiliki peran kunci dalam menghubungkan dunia fisik dengan platform digital, yang

memungkinkan pengumpulan data secara *real-time*.

2. Gateway: komponen ini berfungsi sebagai penghubung antara sensor dan jaringan komunikasi. Ia mengumpulkan data dari sensor yang berada dalam jarak dekat dan mengirimkannya ke *Cloud* melalui jaringan komunikasi yang lebih luas. Gateway juga dapat melakukan pengolahan awal (pre-processing) data sebelum mengirimkannya ke *Cloud* untuk mengurangi beban pemrosesan di *server Cloud*. Menurut (Buyya et al., 2013), gateway memainkan peran penting dalam menangani masalah seperti latensi dan mengatasi keterbatasan sensor dalam hal kekuatan pengolahan dan penyimpanan.
3. Jaringan Komunikasi: komponen ini mencakup semua teknologi komunikasi yang digunakan untuk mentransmisikan data dari sensor ke *Cloud*. Jaringan komunikasi dalam arsitektur Sensor *Cloud* bisa berbasis teknologi nirkabel seperti Wi-Fi, LTE, 5G, ZigBee, atau teknologi wired seperti Ethernet. Jaringan komunikasi yang

andal dan efisien sangat penting untuk memastikan bahwa data sensor dapat dikirimkan dengan cepat dan akurat tanpa gangguan.

4. *Cloud Computing*: Komponen ini menyediakan infrastruktur pemrosesan dan penyimpanan yang skalabel dan dapat diakses dari mana saja. Data sensor yang dikirim melalui jaringan komunikasi akan disimpan, diolah, dan dianalisis di *Cloud*. *Cloud* juga menyediakan layanan untuk berbagai aplikasi berbasis *IoT* yang memerlukan akses ke data ini. Menurut (Gubbi et al., 2013), pemanfaatan *Cloud computing* dalam arsitektur Sensor *Cloud* tidak hanya meningkatkan efisiensi pemrosesan data, tetapi juga memungkinkan pengguna dan sistem untuk mengakses data secara *real-time*.

8.2.2. Lapisan dalam Arsitektur Sensor *Cloud*

1. Lapisan Perangkat (*Device Layer*): Lapisan perangkat merupakan lapisan terendah yang terdiri dari sensor dan aktuator yang berfungsi untuk mendeteksi dan mengukur

perubahan fisik. Data dari perangkat ini dikumpulkan dan dikirimkan melalui gateway ke lapisan berikutnya. Menurut (Atzori et al., 2010), lapisan perangkat berperan dalam mendeteksi kondisi lingkungan, seperti suhu, kelembaban, cahaya, dan tekanan, yang kemudian diolah menjadi informasi yang dapat digunakan oleh aplikasi.

2. Lapisan Jaringan (Network *Layer*): Lapisan jaringan bertanggung jawab untuk mentransmisikan data dari lapisan perangkat ke *Cloud*. Jaringan yang digunakan dalam lapisan ini dapat mencakup teknologi komunikasi seperti Wi-Fi, ZigBee, atau jaringan seluler. Jaringan ini menjembatani komunikasi antara sensor, gateway, dan platform *Cloud*. Lapisan jaringan harus dirancang untuk menjamin keamanan, efisiensi, dan kecepatan transmisi data dalam arsitektur *IoT*.
3. Lapisan Layanan (Service *Layer*): Lapisan layanan adalah tempat di mana data dari sensor diolah menjadi layanan yang dapat

diakses oleh aplikasi. *Cloud computing* berperan besar dalam lapisan ini dengan menyediakan pemrosesan data, analitik, penyimpanan, serta layanan keamanan. (Buyya et al., 2013) menekankan pentingnya lapisan ini dalam mendukung berbagai aplikasi yang membutuhkan informasi *real-time* dari sensor dan juga manajemen data yang baik.

4. Lapisan Aplikasi (Application *Layer*): Lapisan aplikasi berfungsi sebagai antarmuka antara pengguna dan sistem. Di sinilah aplikasi *IoT* berinteraksi dengan data sensor yang telah diolah di *Cloud* untuk menyediakan layanan seperti pemantauan lingkungan, sistem keamanan, atau smart cities. (Gubbi et al., 2013) menekankan bahwa lapisan aplikasi adalah yang paling terlihat oleh pengguna, di mana mereka dapat mengambil manfaat langsung dari data yang dihasilkan oleh jaringan sensor.

8.2.3. Integrasi Sensor dengan *Cloud*: Protokol dan Teknologi

1. Protokol MQTT (*Message Queuing Telemetry Transport*): Protokol MQTT adalah protokol ringan yang sering digunakan untuk komunikasi M2M (*Machine to Machine*) dalam *IoT*. Protokol ini dirancang untuk bekerja dengan jaringan bandwidth rendah dan cocok untuk mengirimkan data dari sensor ke *Cloud* dengan konsumsi daya yang minimal. Menurut (Schneider et al., 2016), MQTT adalah pilihan yang populer karena kesederhanaannya dan efisiensi dalam mengirimkan pesan kecil dari sensor yang memiliki sumber daya terbatas.
2. Protokol CoAP (*Constrained Application Protocol*): Protokol CoAP adalah protokol yang dirancang untuk digunakan dalam lingkungan yang memiliki keterbatasan daya dan bandwidth, seperti jaringan sensor. Protokol ini menggunakan model client-*server* yang serupa dengan HTTP, namun lebih efisien dalam hal pemakaian sumber daya. CoAP sangat cocok untuk

aplikasi *IoT* yang memerlukan komunikasi efisien dan respons cepat, terutama dalam kondisi yang membatasi penggunaan bandwidth dan daya.

3. Teknologi REST API (*Representational State Transfer Application Programming Interface*): REST API digunakan untuk memungkinkan interaksi antara sensor dan *Cloud* melalui *web*. REST API menawarkan cara standar untuk mengakses dan mengelola data sensor melalui HTTP, memungkinkan integrasi yang lebih mudah antara perangkat *IoT* dan layanan *Cloud*. REST API memungkinkan interaksi antar-sistem yang bersifat stateless, yang berarti setiap permintaan dari sensor ke *Cloud* memuat semua informasi yang diperlukan untuk diproses, menjadikannya cocok untuk aplikasi *IoT* yang terdistribusi.

8.3. Fungsi dan Fitur Sensor *Cloud*

Sensor *Cloud* merupakan arsitektur yang memungkinkan integrasi berbagai sensor fisik dengan teknologi *Cloud* untuk pengumpulan, penyimpanan, pemrosesan, dan analisis data. Fungsi-fungsi utama

Sensor *Cloud* mencakup berbagai aspek penting dari manajemen data hingga analitik, yang semuanya memanfaatkan infrastruktur *Cloud* untuk mendukung aplikasi *IoT* (*Internet of Things*).

8.3.1. Pengumpulan Data dari Sensor

Pengumpulan data adalah fungsi utama dari arsitektur Sensor *Cloud*, di mana sensor fisik yang tersebar mengumpulkan informasi dari lingkungan atau sistem tertentu. Data ini mencakup berbagai parameter seperti suhu, kelembaban, tekanan, cahaya, atau bahkan pergerakan. Proses pengumpulan data dapat berlangsung secara *real-time*, dan informasi yang didapat dikirimkan ke *Cloud* melalui jaringan komunikasi seperti Wi-Fi, *Bluetooth*, atau jaringan seluler. Keunggulan utama pengumpulan data dalam Sensor *Cloud* adalah kemampuannya untuk melakukan pemantauan secara kontinu dan *real-time*, memberikan pengguna akses langsung ke data yang terkini.

8.3.2. Penyimpanan dan Pemrosesan Data di *Cloud*

Setelah data dikumpulkan, ia dikirimkan ke *Cloud* untuk penyimpanan dan pemrosesan lebih

lanjut. *Cloud* menawarkan ruang penyimpanan yang hampir tidak terbatas dan infrastruktur pemrosesan yang sangat skalabel, sehingga mampu menangani volume data besar yang dihasilkan oleh jaringan sensor. Pemrosesan ini mencakup penyaringan, agregasi, dan pengolahan data mentah menjadi informasi yang lebih bermakna. Pemanfaatan teknologi *Cloud* dalam pemrosesan data sensor memungkinkan efisiensi yang lebih tinggi, karena sebagian besar beban komputasi diambil alih oleh *server Cloud*, bukan oleh perangkat sensor yang memiliki keterbatasan daya dan kapasitas.

8.3.3. Analitik Data dalam Sensor *Cloud*

Sensor *Cloud* menyediakan kemampuan analitik data yang canggih, di mana data yang telah diproses dapat dianalisis untuk mendeteksi pola, tren, atau anomali tertentu. Analitik ini sangat penting untuk berbagai aplikasi, seperti pemantauan kesehatan, industri, pertanian pintar, dan pengelolaan energi. Algoritma machine learning dan kecerdasan buatan (AI) sering digunakan dalam proses analitik ini untuk memberikan prediksi atau rekomendasi

berdasarkan data yang dikumpulkan. Analitik data dalam Sensor *Cloud* sangat penting untuk aplikasi *IoT* yang memerlukan keputusan *real-time*, misalnya dalam sistem lalu lintas cerdas atau pemantauan lingkungan.

8.3.4. Pengelolaan dan Kontrol Sensor melalui *Cloud*

Fitur lain yang penting dalam Sensor *Cloud* adalah kemampuan untuk mengelola dan mengontrol sensor dari jarak jauh melalui *Cloud*. Platform *Cloud* memungkinkan pengguna untuk memantau status sensor, melakukan konfigurasi ulang, memperbarui firmware, atau bahkan mematikan sensor jika diperlukan. Hal ini membuat sistem lebih fleksibel dan mudah diatur, terutama jika sensor berada di lokasi yang sulit dijangkau. (Atzori et al., 2010) menekankan bahwa kontrol sensor dari jarak jauh melalui *Cloud* tidak hanya meningkatkan efisiensi operasional, tetapi juga memungkinkan pemeliharaan preventif untuk meminimalkan downtime.

8.3.5. Keamanan dan Privasi dalam Sensor *Cloud*

Keamanan dan privasi adalah aspek krusial dalam Sensor *Cloud*, terutama mengingat banyaknya data yang dikumpulkan, disimpan, dan dianalisis. Data sensor sering kali mencakup informasi sensitif, seperti data kesehatan atau data industri kritis. Oleh karena itu, diperlukan mekanisme keamanan yang kuat untuk melindungi data dari akses tidak sah, pencurian, atau serangan siber. Teknologi enkripsi, autentikasi, dan kontrol akses sering digunakan untuk memastikan bahwa hanya pihak yang berwenang yang dapat mengakses data. Isu privasi menjadi semakin penting ketika data dari berbagai perangkat *IoT* dikumpulkan dan diproses dalam jumlah besar, sehingga sistem perlu menerapkan strategi keamanan yang komprehensif untuk menjaga integritas data dan privasi pengguna.

8.4. Teknologi Pendukung Sensor *Cloud*

Teknologi pendukung dalam arsitektur Sensor *Cloud* mencakup berbagai solusi komputasi dan platform *IoT* yang dirancang untuk mengelola data dalam jumlah besar yang dikumpulkan dari sensor.

Dalam bagian ini, akan dijelaskan beberapa teknologi kunci yang memungkinkan Sensor *Cloud* berfungsi secara efektif, mulai dari komputasi awan hingga teknologi *edge* dan fog *computing*.

8.4.1. Teknologi Komputasi Awan (*Cloud Computing*)

Komputasi awan adalah tulang punggung utama dari arsitektur Sensor *Cloud*. Dengan menggunakan teknologi *Cloud*, data yang dikumpulkan dari jaringan sensor dapat disimpan, diproses, dan dianalisis dalam infrastruktur yang skalabel dan elastis. *Cloud computing* memungkinkan penanganan data besar (*big data*), memberikan solusi penyimpanan yang fleksibel, serta mendukung pemrosesan *real-time* untuk aplikasi *IoT*. Salah satu keuntungan utama dari teknologi komputasi awan adalah skalabilitasnya yang memungkinkan sistem Sensor *Cloud* untuk tumbuh tanpa batas, sesuai dengan kebutuhan data dan aplikasi yang terus berkembang. Selain itu, layanan komputasi awan seperti Amazon *Web* Services (AWS), Google *Cloud*, dan Microsoft Azure menawarkan fitur keamanan, manajemen, serta pemrosesan data yang dapat disesuaikan.

8.4.2. Teknologi *Edge* dan *Fog Computing* dalam Sensor *Cloud*

Selain *Cloud computing*, teknologi *edge* dan fog *computing* juga memainkan peran penting dalam arsitektur Sensor *Cloud*, terutama untuk menangani data secara lokal dan mengurangi latensi. *Edge computing* memungkinkan pemrosesan data dilakukan di dekat sumber data, yaitu di perangkat sensor atau gateway, sehingga tidak semua data perlu dikirimkan ke *Cloud* untuk pemrosesan. Fog *computing*, di sisi lain, bekerja sebagai lapisan antara sensor dan *Cloud*, di mana beberapa proses pemrosesan dan penyimpanan dapat dilakukan pada perangkat lokal atau *edge* nodes. *Edge* dan fog *computing* sangat penting dalam aplikasi yang memerlukan respons *real-time*, seperti sistem keamanan, smart cities, atau kendaraan otonom. Teknologi ini membantu mengurangi beban pada *Cloud* dan memastikan bahwa keputusan dapat diambil lebih cepat dan lebih efisien.

8.4.3. *Platform IoT* berbasis Sensor *Cloud*

Beberapa platform *IoT* besar menyediakan layanan Sensor *Cloud* yang terintegrasi dengan

komputasi awan, *edge*, dan fog *computing*. Berikut adalah tiga platform *IoT* terkemuka yang mendukung Sensor *Cloud*:

1. AWS *IoT*: Amazon *Web* Services (AWS) *IoT* Core memungkinkan perangkat *IoT* terhubung dengan aman dan berinteraksi dengan aplikasi *Cloud* lainnya. Platform ini menyediakan layanan manajemen perangkat, pengumpulan data, dan analisis. AWS *IoT* juga mendukung protokol komunikasi *IoT* seperti MQTT, HTTP, dan *Web*Sockets, serta menyediakan infrastruktur komputasi *Cloud* yang tangguh. AWS *IoT* mendukung berbagai kasus penggunaan, termasuk rumah pintar, kendaraan terhubung, dan monitoring industri, di mana sensor dapat dikelola dengan mudah melalui platform *Cloud* ini.
2. Google *Cloud IoT*: Google *Cloud IoT* menyediakan solusi lengkap untuk menghubungkan, mengelola, dan mengamankan perangkat *IoT* di seluruh dunia. Layanan ini menawarkan pengumpulan data secara *real-time*, kemampuan analitik yang kuat, serta

integrasi dengan layanan *big data* dan AI/ML Google, seperti BigQuery dan TensorFlow, untuk analisis lebih mendalam. Google *Cloud IoT* banyak digunakan dalam proyek smart city dan pemantauan lingkungan, di mana volume data yang besar dapat dianalisis untuk membuat keputusan yang berbasis data.

3. Microsoft Azure *IoT*: Microsoft Azure *IoT* Hub adalah platform *IoT* yang memungkinkan perangkat sensor terhubung dengan aman dan bertukar data dengan *Cloud*. Platform ini mendukung berbagai protokol komunikasi, serta menyediakan fitur manajemen perangkat dan analitik data. Selain itu, Azure *IoT* memiliki fitur *edge computing* yang memungkinkan pemrosesan data di dekat perangkat sensor untuk mengurangi latensi. Microsoft Azure *IoT* sering digunakan dalam aplikasi industri seperti manufaktur cerdas, pengelolaan energi, dan pemeliharaan prediktif, di mana integrasi sensor dengan *Cloud* adalah kunci untuk pengumpulan data *real-time*.

8.5. Implementasi dan Kasus Penggunaan Sensor *Cloud*

Sensor *Cloud* memiliki potensi besar untuk diterapkan dalam berbagai sektor karena kemampuannya untuk mengintegrasikan sensor fisik dengan infrastruktur *Cloud* untuk pengumpulan, pemrosesan, dan analisis data secara *real-time*. Berikut adalah implementasi dan beberapa kasus penggunaan utama dari teknologi Sensor *Cloud* dalam berbagai bidang.

8.5.1. Implementasi Sensor *Cloud* dalam Sektor Industri

Di sektor industri, Sensor *Cloud* banyak digunakan dalam Industrial *IoT* (I*IoT*) untuk meningkatkan efisiensi produksi, memantau kondisi mesin, dan mengotomatiskan proses. Dengan menghubungkan sensor ke *Cloud*, perusahaan dapat mengumpulkan data dari berbagai mesin dan perangkat secara *real-time*, yang kemudian dianalisis untuk mendeteksi potensi masalah, seperti kegagalan mesin, atau mengoptimalkan alur kerja. (Buyya et al., 2013) menjelaskan bahwa dengan Sensor *Cloud*, proses seperti prediktif maintenance (pemeliharaan

prediktif) dapat diterapkan. Sensor yang terhubung akan mengumpulkan data operasional dari mesin, yang kemudian dianalisis di *Cloud* untuk mendeteksi kapan komponen tertentu perlu diperbaiki atau diganti. Hal ini mengurangi downtime dan meningkatkan produktivitas.

8.5.2. Sensor *Cloud* di Bidang Pertanian (*Smart Agriculture*)

Sensor *Cloud* juga banyak digunakan dalam pertanian cerdas (smart agriculture). Sensor yang ditempatkan di ladang dapat mengukur berbagai parameter lingkungan seperti suhu, kelembapan tanah, dan kandungan nutrisi. Data ini dikirim ke *Cloud* untuk dianalisis, sehingga petani dapat membuat keputusan berdasarkan data yang akurat, misalnya kapan waktu terbaik untuk irigasi atau pemupukan. Menurut (Patil & Kale, 2016), sensor yang terhubung dengan *Cloud* memungkinkan pengelolaan pertanian secara otomatis dan efisien. Dengan menggunakan data *real-time*, petani dapat mengoptimalkan hasil panen, mengurangi penggunaan air, dan menghindari pemborosan sumber daya.

8.5.3. Sensor *Cloud* di Bidang Kesehatan (*Healthcare IoT*)

Di sektor kesehatan, Sensor *Cloud* mendukung konsep Healthcare *IoT* dengan menghubungkan perangkat medis yang dapat dipakai (wearables) ke *Cloud* untuk memantau kondisi pasien secara *real-time*. Sensor ini dapat mengukur tanda-tanda vital seperti detak jantung, tekanan darah, dan tingkat oksigen dalam darah, yang kemudian dianalisis di *Cloud* untuk mendeteksi pola yang tidak normal atau risiko kesehatan. (Farahani et al., 2018) menekankan pentingnya Sensor *Cloud* dalam layanan kesehatan jarak jauh (telemedicine). Teknologi ini memungkinkan dokter dan penyedia layanan kesehatan untuk memantau pasien dari jarak jauh, mengurangi kebutuhan kunjungan fisik, dan memberikan perawatan preventif melalui analisis data secara *real-time*.

8.5.4. Sensor *Cloud* dalam Sistem Pemantauan Lingkungan (*Environmental Monitoring*)

Sensor *Cloud* memainkan peran kunci dalam pemantauan lingkungan, seperti pengukuran polusi udara, kualitas air, atau perubahan iklim. Sensor

yang ditempatkan di berbagai titik geografis dapat mengirim data ke *Cloud*, di mana informasi ini diproses dan dianalisis untuk memprediksi tren lingkungan atau memberikan peringatan dini terkait bahaya lingkungan seperti banjir atau kebakaran hutan. Menurut (Akan et al., 2010), pemantauan lingkungan berbasis Sensor *Cloud* sangat berguna dalam mitigasi bencana, di mana data dari sensor dapat membantu pemerintah dan lembaga terkait dalam merespons dengan cepat. Sensor ini juga digunakan untuk memantau perubahan lingkungan jangka panjang yang berkaitan dengan perubahan iklim global.

8.5.5. Sensor *Cloud* untuk *Smart City*

Konsep Smart City tidak lepas dari implementasi Sensor *Cloud*, di mana berbagai sensor digunakan untuk mengelola infrastruktur perkotaan secara lebih cerdas dan efisien. Dalam kota pintar, Sensor *Cloud* dapat digunakan untuk memantau lalu lintas, mengelola sistem transportasi umum, memantau kualitas udara, dan mengelola pencahayaan atau penggunaan energi di gedung-gedung. (Gubbi et al., 2013) menyatakan bahwa di kota pintar, sensor yang terhubung

dengan *Cloud* dapat membantu otoritas lokal dalam pengambilan keputusan berbasis data. Sebagai contoh, data dari sensor lalu lintas dapat digunakan untuk mengurangi kemacetan dengan menyesuaikan pengaturan lampu lalu lintas secara *real-time*, sementara sensor kualitas udara dapat membantu dalam pengelolaan polusi udara perkotaan.

8.6. Keamanan dan Privasi dalam Sensor *Cloud*

Keamanan dan privasi menjadi tantangan utama dalam implementasi Sensor *Cloud*, mengingat sifatnya yang melibatkan banyak sensor, jaringan, dan sistem *Cloud*. Dalam konteks *Internet of Things* (*IoT*), di mana Sensor *Cloud* memainkan peran kunci, risiko terhadap keamanan dan privasi pengguna semakin tinggi. Oleh karena itu, mekanisme keamanan yang kuat dan kebijakan privasi yang jelas sangat diperlukan.

8.6.1. Tantangan Keamanan pada Sensor *Cloud*

Sensor *Cloud* menghadapi berbagai tantangan keamanan karena menggabungkan dua teknologi kompleks: sensor yang tersebar secara luas dan infrastruktur *Cloud* yang menjadi pusat pemrosesan data. Tantangan utama meliputi:

1. Serangan pada perangkat sensor: Sensor sering kali ditempatkan di lokasi terpencil dan terbuka, menjadikannya rentan terhadap serangan fisik seperti perusakan, manipulasi, atau pencurian data.
2. Kerentanan jaringan: Jaringan yang menghubungkan sensor dengan *Cloud* menjadi target potensial serangan, termasuk Man-in-the-Middle Attacks, yang memungkinkan peretas mengintersepsi data sebelum mencapai *Cloud*.
3. Keamanan data di *Cloud*: Data yang dikumpulkan oleh sensor sering kali sensitif dan perlu dilindungi dari akses yang tidak sah saat disimpan atau diproses di *Cloud*.

Menurut (Krutz & Vines, 2010), tantangan ini memerlukan pendekatan holistik untuk keamanan yang melibatkan setiap lapisan dalam arsitektur Sensor *Cloud*, mulai dari perangkat sensor hingga jaringan komunikasi dan pusat *Cloud* itu sendiri.

8.6.2. Mekanisme Keamanan untuk Perlindungan Data

Untuk melindungi data sensor di dalam Sensor *Cloud*, ada beberapa mekanisme keamanan yang umum diterapkan:

1. Enkripsi Data: Enkripsi adalah salah satu mekanisme paling penting dalam menjaga kerahasiaan data. Data yang dikirim dari sensor ke *Cloud* dan selama penyimpanan di *Cloud* perlu dienkripsi untuk mencegah akses oleh pihak yang tidak berwenang. Algoritma enkripsi seperti AES (Advanced Encryption Standard) atau RSA digunakan untuk menjaga keamanan data saat transit maupun saat tersimpan. Enkripsi end-to-end memastikan data tetap aman sepanjang perjalanan dari sensor hingga *Cloud*. Enkripsi ini melibatkan kunci yang hanya dapat diakses oleh entitas yang berwenang.
2. Otentikasi dan Otorisasi: Mekanisme otentikasi memastikan bahwa hanya perangkat yang sah dan terverifikasi yang dapat berkomunikasi dengan *Cloud*. Proses otorisasi memastikan bahwa setiap perangkat atau pengguna memiliki izin

yang tepat untuk mengakses sumber daya yang relevan. Teknik seperti sertifikat digital dan token otentikasi sering digunakan untuk mengamankan akses.

3. Firewall dan IDS/IPS (Intrusion Detection System/Intrusion Prevention System): Firewall berfungsi sebagai lapisan pertahanan untuk melindungi jaringan dari serangan luar, sementara IDS/IPS digunakan untuk mendeteksi dan mencegah serangan yang berhasil melewati firewall. IDS mengidentifikasi aktivitas mencurigakan dan memberi peringatan, sedangkan IPS secara aktif memblokir atau mengurangi dampak serangan. (Rittinghouse & Ransome, 2016) menjelaskan bahwa kombinasi firewall dan IDS/IPS memberikan lapisan perlindungan tambahan terhadap ancaman yang berkembang, terutama di lingkungan yang melibatkan koneksi sensor ke *Cloud*.

8.6.3. Privasi Data Sensor di *Cloud*

Privasi data menjadi isu kritis karena data yang dikumpulkan oleh sensor sering kali bersifat

pribadi dan dapat mencakup informasi yang sangat sensitif, seperti data kesehatan, lokasi, atau kebiasaan pengguna. Untuk menjaga privasi data sensor di *Cloud*, beberapa langkah dapat diambil:

1. Anonimisasi Data: Data yang dikirim ke *Cloud* dapat dianonimkan sehingga informasi pribadi pengguna tidak dapat dilacak kembali ke identitas asli.
2. Kontrol Akses Berbasis Kebijakan: Pengguna dan organisasi dapat menetapkan kebijakan untuk mengontrol siapa yang memiliki akses ke data sensor tertentu, dengan memastikan bahwa hanya individu atau entitas yang berwenang yang dapat mengakses informasi sensitif.

(Zhou et al., 2018) menyebutkan bahwa teknik enkripsi dan anonimisasi yang tepat dapat melindungi privasi pengguna dalam sistem berbasis Sensor *Cloud*, sementara pengaturan kebijakan akses yang ketat dapat memastikan bahwa privasi tetap terjaga.

8.6.4. Studi Kasus Ancaman Keamanan pada Sensor *Cloud*

Beberapa ancaman keamanan yang sering terjadi pada implementasi Sensor *Cloud* mencakup:

1. Serangan Distributed Denial of Service (DDoS): Sensor *Cloud* sering menjadi target serangan DDoS, di mana lalu lintas data yang tidak normal menyebabkan *server Cloud* menjadi tidak responsif. Ini sering terjadi karena banyaknya perangkat *IoT* yang terhubung ke *Cloud*, sehingga memperbesar skala potensi serangan.
2. Data Breach: Salah satu kasus paling terkenal adalah kebocoran data yang melibatkan sensor kesehatan yang terhubung ke *Cloud*. Data medis yang dikumpulkan oleh sensor ini disusupi dan diakses oleh pihak yang tidak sah, menyebabkan pelanggaran privasi pasien.

Serangan semacam ini menunjukkan betapa pentingnya memiliki protokol keamanan yang kuat dan terus diperbarui untuk melindungi data sensor di *Cloud*. Ancaman ini juga menyoroti perlunya

pemantauan yang konstan dan respons cepat terhadap insiden keamanan.

BAB IX
INDUSTRIAL *IOT*

9.1. Konsep Dasar Industrial *IoT*

Definisi Industrial *IoT* (I*IoT*)

Industrial *IoT* (I*IoT*) adalah aplikasi *Internet of Things* (*IoT*) yang diterapkan dalam lingkungan industri untuk meningkatkan efisiensi, produktivitas, dan pemantauan proses industri. I*IoT* melibatkan penggunaan sensor, perangkat cerdas, dan teknologi komunikasi untuk mengumpulkan, mengirim, dan menganalisis data dari mesin, perangkat, dan sistem yang ada di fasilitas industri. Tujuan utama dari I*IoT* adalah untuk memberikan wawasan *real-time* tentang operasi industri, mengoptimalkan proses, mengurangi biaya, dan meningkatkan keselamatan serta keandalan.

Ciri-ciri I*IoT* termasuk:

- Sensor dan Aktuator: Perangkat yang terpasang pada mesin dan peralatan industri untuk mengumpulkan data dan melakukan tindakan otomatis.
- Data Analytics: Menggunakan algoritma analitik untuk memproses data yang dikumpulkan dan menghasilkan wawasan yang berguna.

- Konektivitas: Menghubungkan berbagai perangkat dan sistem melalui jaringan untuk berbagi data secara efisien.
- *Cloud Computing* dan *Edge Computing*: Mengelola dan menganalisis data baik di *Cloud* maupun di *edge* (dekat dengan sumber data) untuk meningkatkan responsivitas dan efisiensi.

Perbedaan antara *IoT* dan I*IoT*

1. Konteks Penggunaan:
    - *IoT* (*Internet of Things*): Umumnya merujuk pada aplikasi *IoT* dalam kehidupan sehari-hari dan konsumer, seperti smart home, wearable devices, dan perangkat cerdas untuk konsumen.
    - I*IoT* (Industrial *Internet of Things*): Fokus pada aplikasi *IoT* dalam lingkungan industri, seperti pabrik, fasilitas energi, dan infrastruktur kritis. I*IoT* dirancang untuk meningkatkan proses industri, efisiensi operasional, dan pengelolaan fasilitas.
2. Skala dan Kompleksitas:
    - *IoT*: Biasanya melibatkan sistem yang lebih kecil dan lebih sederhana dengan

fokus pada kebutuhan konsumen, seperti perangkat rumah pintar atau wearable.

- I*IoT*: Melibatkan sistem yang lebih kompleks dan berskala besar, dengan fokus pada integrasi dan manajemen sistem industri yang besar dan sering kali kritis.

3. Jenis Data:
    - *IoT*: Mengumpulkan data yang berkaitan dengan kebiasaan konsumen, kesehatan pribadi, dan interaksi sehari-hari.
    - I*IoT*: Mengumpulkan data operasional yang berkaitan dengan mesin, proses produksi, kondisi lingkungan industri, dan parameter teknis yang mempengaruhi kinerja sistem industri.
4. Tujuan Utama:
    - *IoT*: Meningkatkan kenyamanan, efisiensi, dan pengalaman pengguna dalam konteks konsumer.
    - I*IoT*: Meningkatkan efisiensi operasional, keandalan, keselamatan, dan penghematan biaya dalam konteks industri.

5. Keamanan dan Regulasi:
    - *IoT*: Keamanan lebih fokus pada perlindungan data pribadi dan privasi pengguna.
    - I*IoT*: Memerlukan tingkat keamanan yang lebih tinggi untuk melindungi data industri dan mencegah gangguan operasional yang dapat berdampak pada keselamatan dan produktivitas.

9.2. Teknologi Kunci dalam Industrial *IoT*

Berikut adalah beberapa teknologi kunci dalam Industrial *IoT* (I*IoT*):

1. *Big data* dan Analitik:
    a. *Big data*: Dalam konteks I*IoT*, *big data* merujuk pada volume besar data yang dikumpulkan dari berbagai sensor, mesin, dan perangkat dalam lingkungan industri. Data ini dapat mencakup informasi tentang kinerja mesin, kondisi lingkungan, dan parameter operasional lainnya.
    b. Analitik: Analitik digunakan untuk memproses dan menganalisis data besar tersebut. Dengan menggunakan

algoritma analitik, data dapat diubah menjadi wawasan yang berguna, seperti mendeteksi pola, memprediksi kegagalan mesin, dan mengidentifikasi peluang untuk efisiensi operasional. Teknik analitik termasuk analisis prediktif, analisis deskriptif, dan analisis preskriptif.

2. Kecerdasan Buatan (AI) dan Machine Learning:
    a. AI dan Machine Learning: AI dan machine learning adalah teknologi yang memungkinkan sistem I*IoT* untuk belajar dari data dan meningkatkan kinerjanya seiring waktu. Dalam I*IoT*, machine learning digunakan untuk menganalisis data industri secara otomatis dan mengidentifikasi pola yang mungkin tidak terlihat oleh manusia. Ini termasuk deteksi anomali, pemeliharaan prediktif, dan optimasi proses.
    b. AI: AI memungkinkan sistem untuk membuat keputusan otomatis berdasarkan data yang dikumpulkan. Misalnya, AI dapat digunakan untuk

mengoptimalkan jadwal pemeliharaan mesin berdasarkan prediksi kegagalan.

3. Jaringan 5G dan Komunikasi Nirkabel:
    a. Jaringan 5G: Jaringan 5G menawarkan kecepatan transfer data yang lebih tinggi, latensi rendah, dan kapasitas koneksi yang lebih besar dibandingkan dengan generasi sebelumnya. Ini memungkinkan komunikasi *real-time* yang lebih baik antara perangkat *IoT* dan sistem pusat, mendukung aplikasi industri yang memerlukan waktu respons cepat dan volume data besar.
    b. Komunikasi Nirkabel: Teknologi komunikasi nirkabel seperti Wi-Fi, LoRaWAN (Long Range Wide Area Network), dan Zigbee digunakan untuk menghubungkan perangkat *IoT* dalam jaringan industri. Pilihan teknologi nirkabel bergantung pada kebutuhan spesifik aplikasi, seperti jangkauan, daya, dan kecepatan data.
4. Teknologi Blockchain:

    Blockchain: Blockchain digunakan untuk menciptakan catatan transaksi yang aman,

transparan, dan tidak dapat diubah. Dalam I*IoT*, blockchain dapat digunakan untuk melacak dan memverifikasi transaksi dalam rantai pasokan, memastikan integritas data, dan meningkatkan keamanan. Misalnya, blockchain dapat membantu memastikan keaslian dan integritas data yang dikumpulkan dari sensor industri.

5. *Cloud Computing* dan *Edge Computing*:
    a. *Cloud Computing*: *Cloud computing* menyediakan infrastruktur dan layanan yang memungkinkan penyimpanan dan pemrosesan data besar dari perangkat I*IoT*. Ini memungkinkan skalabilitas dan fleksibilitas dalam mengelola dan menganalisis data industri tanpa memerlukan infrastruktur lokal yang besar.
    b. *Edge Computing*: *Edge computing* melibatkan pemrosesan data dekat dengan sumber data, yaitu di "*edge*" jaringan. Ini mengurangi latensi dan meningkatkan kecepatan respons dengan memproses data secara lokal sebelum mengirimkan hasilnya ke *Cloud*. *Edge computing* sangat penting untuk

aplikasi yang memerlukan analisis *real-time* dan keputusan cepat.

6. Sensor dan Aktuator:
    a. Sensor: Sensor adalah perangkat yang mengukur parameter fisik atau lingkungan, seperti suhu, tekanan, kelembapan, dan getaran, dan mengirimkan data tersebut ke sistem pusat. Sensor adalah komponen utama dalam I*IoT* yang menyediakan data yang diperlukan untuk pemantauan dan analisis.
    b. Aktuator: Aktuator adalah perangkat yang menerima sinyal dari sistem I*IoT* dan melakukan tindakan fisik, seperti mengendalikan katup, motor, atau aktuator lainnya. Mereka memungkinkan sistem untuk berinteraksi dengan dunia fisik berdasarkan data yang dikumpulkan dan dianalisis.

Teknologi-teknologi ini bekerja sama untuk menciptakan solusi I*IoT* yang efisien, terhubung, dan

cerdas, memungkinkan industri untuk meningkatkan kinerja, efisiensi, dan keselamatan.

9.3. Standar dan Regulasi Industrial *IoT* (I*IoT*)

Standar dan regulasi dalam Industrial *IoT* (I*IoT*) penting untuk memastikan interoperabilitas, keamanan, dan kepatuhan dalam penerapan teknologi I*IoT* di industri. Berikut adalah beberapa aspek utama terkait standar dan regulasi I*IoT*:

1. Standar Internasional
    a. Standar Komunikasi dan Interoperabilitas
        - ISO/IEC 30141 (*Internet of Things* Reference Architecture): Standar ini menyediakan arsitektur referensi untuk *IoT*, termasuk I*IoT*, dengan fokus pada aspek interoperabilitas antara berbagai sistem dan perangkat *IoT*.
        - IEEE 802.15 (Wireless Personal Area Networks): Kumpulan standar ini mencakup berbagai protokol komunikasi nirkabel yang digunakan dalam I*IoT*, termasuk Zigbee dan *Bluetooth* Low Energy (BLE), yang penting untuk komunikasi antara perangkat *IoT*.

- OPC UA (Open Platform Communications Unified Architecture): Standar ini menyediakan protokol komunikasi untuk interoperabilitas antara perangkat industri dan sistem kontrol. OPC UA adalah standar penting dalam I*IoT* karena memungkinkan data dari berbagai perangkat dan sistem untuk saling berkomunikasi dengan aman.

b. Standar Data dan Semantik
   - ISO/IEC 20922 (MQTT - Message Queuing Telemetry Transport): MQTT adalah protokol komunikasi yang digunakan untuk transfer data dalam lingkungan *IoT*, termasuk I*IoT*. Standar ini mendefinisikan cara data dikirim secara efisien antara perangkat *IoT*.
   - ISO/IEC 18295-1 (Data Models for Industrial *IoT*): Standar ini membahas model data untuk sistem industri yang terhubung, memastikan konsistensi dan interoperabilitas dalam pengelolaan data.

2. Regulasi Keamanan dan Kepatuhan

a. Regulasi Keamanan
    - NIST Cybersecurity Framework (CSF): Framework ini dikembangkan oleh National Institute of Standards and Technology (NIST) untuk membantu organisasi dalam mengelola risiko keamanan siber. Dalam konteks I*IoT*, framework ini membantu mengidentifikasi, melindungi, mendeteksi, merespons, dan memulihkan dari ancaman keamanan.
    - GDPR (General Data Protection Regulation): Regulasi ini berlaku di Uni Eropa dan mengatur perlindungan data pribadi. Dalam konteks I*IoT*, GDPR mempengaruhi bagaimana data pribadi dikumpulkan, disimpan, dan digunakan oleh perangkat dan sistem *IoT*.
b. Regulasi Kepatuhan
    - ISO/IEC 27001 (Information Security Management Systems): Standar ini menetapkan persyaratan untuk sistem manajemen keamanan informasi, termasuk pengelolaan risiko yang

terkait dengan data yang dikumpulkan dan diproses oleh perangkat I*IoT*.

- FDA (Food and Drug Administration) Regulations: Untuk industri kesehatan, FDA memiliki regulasi khusus terkait perangkat medis dan kesehatan yang terhubung, termasuk perangkat I*IoT*, untuk memastikan kepatuhan terhadap standar keamanan dan efektivitas.

3. Inisiatif dan Konsorsium I*IoT*
   a. Industrial Internet Consortium (IIC): Konsorsium ini berfokus pada pengembangan standar dan praktik terbaik untuk I*IoT*. Mereka bekerja pada berbagai aspek termasuk arsitektur, interoperabilitas, dan keamanan dalam penerapan teknologi I*IoT*.
   b. Industrial Automation and Control Systems Security (IACSS): Inisiatif ini berfokus pada pengembangan standar dan pedoman untuk keamanan sistem kontrol industri dan otomatisasi yang juga mencakup teknologi I*IoT*.
4. Standar Industri Terkait

a. IEC 62443 (Industrial Communication Networks - Network and System Security): Standar ini menyediakan panduan untuk keamanan sistem dan jaringan industri, mencakup aspek penting dari I*IoT* dalam melindungi infrastruktur industri dari ancaman siber.
b. ISO/TS 15066 (Collaborative Robots): Standar ini mengatur keamanan dan interaksi antara robot kolaboratif dan manusia dalam lingkungan industri, yang relevan dalam konteks penerapan robotik dalam I*IoT*.

Standar dan regulasi dalam I*IoT* memainkan peran penting dalam memastikan bahwa implementasi teknologi ini dilakukan dengan cara yang aman, efisien, dan interoperabel. Mereka membantu memastikan bahwa perangkat dan sistem I*IoT* dapat berfungsi secara harmonis, mematuhi persyaratan keamanan, dan memenuhi standar industri yang relevan.

BAB X
KASUS *IOT*

10.1. Kasus *IoT* dalam Sektor Kesehatan

IoT (*Internet of Things*) dalam sektor kesehatan merujuk pada penerapan teknologi *IoT* untuk meningkatkan perawatan kesehatan, efisiensi operasional, dan pengalaman pasien. Teknologi ini memungkinkan pengumpulan dan analisis data kesehatan secara *real-time*, yang membantu dalam pemantauan, diagnosis, dan perawatan. Berikut adalah beberapa kasus dan aplikasi utama *IoT* dalam sektor kesehatan:

1. Pemantauan Kesehatan Jarak Jauh

   Pemantauan kesehatan jarak jauh menggunakan perangkat *IoT* memungkinkan pasien untuk memantau kondisi kesehatan mereka di rumah dan mengirimkan data ke penyedia layanan kesehatan tanpa perlu kunjungan fisik. Ini termasuk penggunaan perangkat seperti monitor tekanan darah, glukometer, dan alat pemantauan detak jantung.

   Contoh:

Fitbit dan Apple Watch: Perangkat wearable ini mengumpulkan data kesehatan seperti detak jantung, aktivitas fisik, dan pola tidur, yang dapat diakses oleh penyedia layanan kesehatan untuk analisis lebih lanjut.

2. Sistem Manajemen Rumah Sakit

   Sistem manajemen rumah sakit berbasis *IoT* mengintegrasikan berbagai teknologi untuk mengelola fasilitas rumah sakit secara efisien. Ini termasuk sistem pelacakan aset, manajemen inventaris, dan pemantauan lingkungan.

   Contoh:

   Sistem Tracking Aset: Menggunakan RFID dan sensor untuk melacak peralatan medis, obat-obatan, dan barang-barang penting lainnya di rumah sakit.

3. Wearable Devices dan Health Tracking

   Perangkat wearable *IoT* dirancang untuk mengumpulkan data kesehatan secara kontinu dari pengguna. Data ini termasuk aktivitas fisik, detak jantung, pola tidur, dan indikator kesehatan lainnya.

   Contoh:

Smart Patches: Patch yang dapat dipakai pada kulit untuk memantau parameter kesehatan seperti glukosa darah atau hidrasi tubuh.

10.2. Kasus *IoT* dalam Sektor Transportasi

IoT (*Internet of Things*) dalam sektor transportasi mencakup penerapan teknologi *IoT* untuk meningkatkan efisiensi, keamanan, dan kenyamanan dalam sistem transportasi. Dengan menggunakan sensor, perangkat komunikasi, dan data analitik, teknologi *IoT* memungkinkan pengelolaan lalu lintas yang lebih baik, kendaraan terhubung, dan sistem transportasi cerdas. Berikut adalah beberapa kasus dan aplikasi utama *IoT* dalam sektor transportasi:

1. Kendaraan Terhubung dan Otonom

   Kendaraan terhubung menggunakan teknologi *IoT* untuk berkomunikasi dengan kendaraan lain, infrastruktur jalan, dan sistem pusat. Ini memungkinkan fitur seperti navigasi yang lebih baik, deteksi tabrakan, dan pengendalian otomatis. Kendaraan otonom, yang merupakan evolusi dari kendaraan terhubung, menggunakan sensor dan algoritma AI untuk mengemudi tanpa intervensi manusia.

   Contoh:

Tesla Autopilot: Sistem pengemudian otomatis Tesla menggunakan sensor dan kamera untuk memantau lingkungan sekitar dan membuat keputusan pengemudian secara *real-time*.

2. Manajemen Lalu Lintas dan Parkir Cerdas

   Sistem manajemen lalu lintas berbasis *IoT* memantau dan mengelola arus lalu lintas secara *real-time* untuk mengurangi kemacetan dan meningkatkan keselamatan. Sistem parkir cerdas menggunakan sensor untuk mengidentifikasi ketersediaan tempat parkir dan membantu pengemudi menemukan tempat parkir dengan lebih efisien.

   Contoh:

   Smart Traffic Lights: Lampu lalu lintas yang terhubung menggunakan sensor untuk mengatur waktu sinyal berdasarkan kepadatan lalu lintas, mengurangi kemacetan dan meningkatkan aliran lalu lintas.

3. Pemantauan dan Perawatan Kendaraan

   Teknologi *IoT* memungkinkan pemantauan kondisi kendaraan secara *real-time*, termasuk kesehatan mesin, tingkat bahan bakar, dan kebutuhan perawatan. Data ini membantu

dalam pemeliharaan prediktif dan perbaikan kendaraan.

Contoh:

Telematics Systems: Sistem telematics seperti OnStar mengumpulkan data dari kendaraan dan mengirimkannya ke pusat layanan untuk analisis, termasuk pemantauan kesehatan kendaraan dan lokasi GPS.

10.3. Kasus *IoT* dalam *Smart Cities*

IoT (*Internet of Things*) dalam konteks smart cities merujuk pada penggunaan teknologi *IoT* untuk meningkatkan kualitas hidup, efisiensi, dan keberlanjutan kota. Smart cities menggunakan perangkat dan sensor *IoT* untuk mengumpulkan data *real-time* dari berbagai sistem kota, seperti transportasi, energi, dan infrastruktur, untuk mengoptimalkan pengelolaan sumber daya dan layanan publik. Berikut adalah beberapa kasus dan aplikasi utama *IoT* dalam smart cities:

1. Infrastruktur Cerdas dan Pengelolaan Energi

   Teknologi *IoT* digunakan untuk memantau dan mengelola infrastruktur kota, termasuk sistem pencahayaan jalan, pengelolaan energi, dan sistem distribusi air. Dengan sensor dan analitik

data, kota dapat mengurangi konsumsi energi, memelihara infrastruktur secara efisien, dan mengurangi dampak lingkungan.

Contoh:

Smart Lighting: Sistem pencahayaan jalan yang terhubung menggunakan sensor untuk menyesuaikan intensitas cahaya berdasarkan kebutuhan, seperti kepadatan lalu lintas dan waktu malam, mengurangi konsumsi energi dan biaya operasional.

2. Sistem Pencahayaan dan Pengelolaan Sampah

   IoT digunakan untuk meningkatkan efisiensi sistem pencahayaan kota dan pengelolaan sampah. Sensor terhubung mengumpulkan data untuk mengoptimalkan penggunaan sumber daya dan mengurangi biaya operasional.

   Contoh:

   Smart Waste Management: Sistem pengelolaan sampah yang menggunakan sensor untuk memantau tingkat pengisian tempat sampah dan mengoptimalkan rute pengumpulan sampah, mengurangi frekuensi pengumpulan dan biaya operasional.

3. Keamanan dan Pengawasan Publik

Sistem pengawasan kota berbasis *IoT* meningkatkan keamanan publik dengan menggunakan kamera CCTV terhubung dan sensor untuk memantau aktivitas dan mendeteksi ancaman. Data yang dikumpulkan digunakan untuk merespons insiden secara cepat dan efektif.

Contoh:

Smart Surveillance Systems: Kamera pengawas yang dilengkapi dengan analitik video untuk mendeteksi perilaku mencurigakan dan memberikan peringatan dini kepada petugas keamanan.

10.4. Kasus *IoT* dalam Industri Manufaktur

IoT (*Internet of Things*) dalam industri manufaktur merujuk pada penggunaan teknologi *IoT* untuk meningkatkan efisiensi operasional, produktivitas, dan kualitas dalam proses produksi. Teknologi ini memungkinkan pemantauan dan pengendalian mesin dan peralatan secara *real-time*, serta pengumpulan data untuk analitik dan perawatan prediktif. Berikut adalah beberapa kasus dan aplikasi utama *IoT* dalam industri manufaktur:

1. Pemantauan dan Otomatisasi Proses Produksi

IoT memungkinkan pemantauan dan kontrol proses produksi secara *real-time* menggunakan sensor yang terhubung. Data yang dikumpulkan dari mesin dan peralatan dapat digunakan untuk mengoptimalkan proses produksi, meningkatkan kualitas produk, dan mengurangi downtime.

Contoh:

Manufacturing Execution Systems (MES): MES yang terintegrasi dengan *IoT* mengumpulkan data dari lini produksi untuk mengoptimalkan jadwal produksi, memantau kinerja mesin, dan mengidentifikasi potensi masalah.

2. Pemeliharaan Prediktif dan Manajemen Rantai Pasokan

   IoT mendukung pemeliharaan prediktif dengan memantau kondisi peralatan secara *real-time*, memungkinkan perusahaan untuk melakukan perawatan sebelum terjadi kerusakan. Selain itu, *IoT* membantu dalam manajemen rantai pasokan dengan memantau inventaris dan aliran material.

   Contoh:

   Predictive Maintenance: Sensor *IoT* memantau kondisi mesin seperti getaran, suhu, dan

tekanan untuk mengidentifikasi tanda-tanda kerusakan sebelum mesin mengalami kegagalan, mengurangi waktu henti dan biaya perbaikan.

3. Integrasi Sistem dan Analitik Data

   IoT memungkinkan integrasi berbagai sistem dalam lingkungan manufaktur dan analisis data besar untuk mendapatkan wawasan yang lebih dalam tentang operasi dan kinerja. Analitik data membantu dalam pengambilan keputusan yang lebih baik dan perbaikan berkelanjutan.

   Contoh:

   Data Integration Platforms: Platform yang mengintegrasikan data dari berbagai sumber (mesin, sensor, ERP) untuk memberikan gambaran menyeluruh tentang operasi pabrik dan mendukung keputusan berbasis data.

10.5. Kasus *IoT* dalam Pertanian

IoT (*Internet of Things*) dalam pertanian, sering disebut sebagai pertanian cerdas atau smart agriculture, mengacu pada penggunaan teknologi *IoT* untuk meningkatkan produktivitas, efisiensi, dan keberlanjutan dalam praktik pertanian. Teknologi ini memungkinkan pemantauan dan pengendalian elemen-

elemen pertanian secara *real-time*, serta pengumpulan dan analisis data untuk pengambilan keputusan yang lebih baik. Berikut adalah beberapa kasus dan aplikasi utama *IoT* dalam pertanian:

1. Pemantauan Tanah dan Kualitas Air

   Sensor *IoT* digunakan untuk memantau kondisi tanah dan kualitas air, termasuk kelembapan, pH, suhu, dan kadar nutrisi. Data ini membantu petani mengelola sumber daya dengan lebih efisien dan memaksimalkan hasil panen.

   Contoh:

   Soil Moisture Sensors: Sensor yang mengukur kelembapan tanah secara *real-time*, memungkinkan petani untuk melakukan irigasi yang lebih tepat waktu dan mengurangi pemborosan air.

2. Sistem Irigasi Cerdas

   Sistem irigasi berbasis *IoT* otomatis mengelola penyiraman tanaman dengan menggunakan data dari sensor kelembapan tanah dan ramalan cuaca. Ini membantu dalam pengelolaan air yang efisien dan mengurangi konsumsi air.

   Contoh:

   Smart Irrigation Systems: Sistem ini menggunakan data dari sensor tanah dan cuaca

untuk mengatur jadwal dan durasi penyiraman secara otomatis, mengoptimalkan penggunaan air dan meningkatkan hasil panen.

3. Pemantauan Kesehatan Tanaman dan Hewan

   Teknologi *IoT* digunakan untuk memantau kesehatan tanaman dan hewan secara *real-time*, mendeteksi penyakit atau infestasi lebih awal, dan mengelola kondisi kesehatan mereka dengan lebih efektif.

   Contoh:

   Crop Health Monitoring: Sensor dan kamera yang memantau kondisi tanaman, mendeteksi gejala penyakit atau kekurangan nutrisi, dan memberikan peringatan kepada petani untuk tindakan preventif.

10.6. Kasus *IoT* dalam *Retail* dan *E-Commerce*

IoT (*Internet of Things*) dalam retail dan e-commerce merujuk pada penggunaan teknologi *IoT* untuk meningkatkan pengalaman pelanggan, efisiensi operasional, dan manajemen rantai pasokan di sektor ritel dan perdagangan elektronik. Dengan menggunakan sensor, perangkat komunikasi, dan analitik data, teknologi *IoT* membantu retailer dan e-commerce dalam mengoptimalkan operasi dan

memberikan layanan yang lebih baik. Berikut adalah beberapa kasus dan aplikasi utama *IoT* dalam retail dan e-commerce:

1. Manajemen Inventaris dan Rantai Pasokan

   Teknologi *IoT* digunakan untuk memantau dan mengelola inventaris secara *real-time*, serta mengoptimalkan rantai pasokan. Sensor *IoT* melacak lokasi dan kondisi barang, membantu dalam mengurangi kelebihan stok dan kekurangan stok, serta memperbaiki efisiensi distribusi.

   Contoh:

   Smart Shelves: Rak yang dilengkapi dengan sensor untuk memantau ketersediaan produk dan memberikan peringatan ketika stok rendah, membantu dalam pengelolaan inventaris yang lebih efisien.

2. Pengalaman Pelanggan yang Ditingkatkan

   IoT digunakan untuk meningkatkan pengalaman pelanggan dengan menyediakan layanan yang lebih personal dan interaktif. Sensor dan perangkat *IoT* memungkinkan retailer untuk menawarkan pengalaman belanja yang lebih baik dan relevan.

   Contoh:

Smart Fitting Rooms: Kamar pas yang dilengkapi dengan teknologi *IoT* yang memungkinkan pelanggan untuk melihat produk dalam berbagai warna atau ukuran secara virtual, serta meminta bantuan staf melalui sistem yang terhubung.

3. Pengelolaan Energi dan Efisiensi Operasional

   IoT membantu retailer dalam mengelola energi dan efisiensi operasional dengan memantau penggunaan energi dan kondisi peralatan secara *real-time*. Ini membantu dalam mengurangi biaya operasional dan jejak karbon.

   Contoh:

   Smart Lighting: Sistem pencahayaan yang terhubung dengan sensor untuk menyesuaikan intensitas cahaya berdasarkan waktu atau kepadatan pelanggan, mengurangi konsumsi energi dan biaya operasional.

DAFTAR PUSTAKA

Akan, O. B., Akyildiz, I. F., & Stojmenovic, I. (2010). Wireless sensor networks: Sensor *Cloud* applications. . IEEE Communications Magazine, 48(8), 92–98.

Andaria, A. C. (2024). Sensor dan Aktuator pada *IoT*. In *Internet of Things*: Konsep dan Implementasinya (pp. 51–63). Get Press Indonesia. https://www.researchgate.net/publication/383977141_Sensor_dan_Aktuator_pada_*IoT*

Anggy Giri Prawiyogi and Aang Solahudin Anwar (2023) 'Perkembangan *Internet of Things* (*IoT*) pada Sektor Energi: Sistematik Literatur Review', Jurnal MENTARI: Manajemen, Pendidikan dan Teknologi Informasi, 1(2), pp. 187–197. Available at: https://doi.org/10.34306/mentari.v1i2.254.

Atzori, L., Iera, A., & Morabito, G. (2010). "The *Internet of Things*: A Survey." Computer Networks, 54(15), 2787-2805.

Atzori, L., Iera, A., & Morabito, G. (2010). The *Internet of Things*: A survey. Computer Networks, 54(15), 2787–2805.

Banks, A., & Gupta, R. (2014). MQTT Version 3.1.1. OASIS Standard.

Bertoldi, P., & Boza-Kiss, B. (2022). "Energy Efficiency in *IoT* Networks: Challenges and Best Practices."

Journal of Network and Computer Applications, 182, 103256.

Bkheet, S.A. and Agbinya, J.I. (2021) 'A Review of Identity Methods of *Internet of Things* (*IOT*)', Advances in *Internet of Things*, 11(04), pp. 153–174. Available at: https://doi.org/10.4236/ait.2021.114011.

Borgia, E. (2014). The *Internet of Things* Vision: Key Features, Applications, and Open Issues. Computer Communications, 54, 1-31.

Budiyanti, R. T. (2021) Buku Ajar *Internet of Things*.

Buyya, R., Broberg, J., & Goscinski, A. M. (2013). *Cloud Computing*: Principles and Paradigms. John Wiley & Sons.

Buyya, R., Vecchiola, C., & Selvi, S. T. (2013). Mastering *Cloud Computing*. McGraw-Hill.

Chen, Y., Zhang, Y., Liu, W., & Shen, Y. (2014). *Cloud computing* security; Fundamentals, mechanisms, and applications. CRC Press.

Cholilalah, Rois Arifin, A. I. H. (2019) 'Fundamental *Internet of Things* (*IOT*) TEORI DAN APLIKASI', Angewandte Chemie International Edition, 6(11), 951–952., pp. 82–95.

Fadillah, A.Z. and Gunawan, R. (2024) 'Potensi *IoT* dalam Industri 4.0', JATI (Jurnal Mahasiswa Teknik Informatika), 8(2), pp. 1932–1940.

Farahani, B., Firouzi, F., & Chakrabarty, K. (2018). Healthcare *IoT*. In Intelligent *Internet of Things*. Springer.

Ferdiansyah Zulkifli, H. N. (2022) *INTERNET OF THINGS* (*IOT*) MEDIA PEMBELAJARAN PRAKTIKUM ERA 4.0, *Internet of Things* (*IoT*) Media Pembelajaran Praktikum Era 4.0.

Fielding, R. T., & Reschke, J. (2014). Hypertext Transfer Protocol (HTTP/1.1): Semantics and Content. IETF RFC 7231.

Forrester Research. (2020). The Future of Retail Technology: *IoT* and Beyond

García-Valls, M., Dubey, A. and Botti, V. (2018) 'Introducing the new paradigm of Social Dispersed *Computing*: Applications, Technologies and Challenges', Journal of Systems Architecture, 91(June), pp. 83–102. Available at: https://doi.org/10.1016/j.sysarc.2018.05.007.

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.

IBM (2024) Apa itu *Internet of Things* (*IoT*)?

Industrial Internet Consortium (IIC). (2021). Industrial Internet Security Framework.

IOT: From Smart Cities to Smart Homes. (2021). John Wiley & Sons.

Javaid, M. et al. (2021) 'Sensors for Daily Life: A Review', Sensors International, 2(July), p. 100121. Available at: https://doi.org/10.1016/j.sintl.2021.100121.

Krutz, R. L., & Vines, R. D. (2010). *Cloud* Security: A Comprehensive Guide to Secure *Cloud Computing*. Wiley Publishing.

Marinos, A., & Briscoe, G. (2009). *Community Cloud Computing*. *Cloud Computing*, 472-484.

McKinsey & Company. (2020). The Next Normal in Manufacturing: How to Rebuild Operations for the Future.

Mell, P., & Grance, T. (2011). The NIST Definition of *Cloud Computing*. National Institute of Standards and Technology.

Minerva, R., Biru, A., & Rotondi, D. (2015). Towards a Definition of the *Internet of Things* (*IoT*). IEEE Internet Initiative.

Miorandi, D., Sicari, S., De Pellegrini, F., & Deriu, S. (2012). "*Internet of Things*: Vision, Applications and Research Challenges." Ad Hoc Networks, 10(7), 1497-1516.

Mollah, M. B., Azad, M. A. K., & & Vasilakos, A. V. (2017). Security and privacy challenges in mobile *Cloud computing*: Survey and way ahead. Journal of Network and Computer Applications, 84, 38–54.

Najib, W., Sulistyo, S. and Widyawan (2020) 'Tinjauan Ancaman dan Solusi Keamanan pada Teknologi *Internet of Things*', Jurnal Nasional Teknik Elektro

dan Teknologi Informasi, 9(4), pp. 375–384. Available at: https://doi.org/10.22146/jnteti.v9i4.539.

NIST. (2018). Framework for Improving Critical Infrastructure Cybersecurity. National Institute of Standards and Technology.

OASIS. (2014). Advanced Message Queuing Protocol (AMQP) 1.0 Specification. OASIS Standard.

Patil, P., & Kale, S. (2016). *IoT* based smart agriculture monitoring and automatic irrigation system. International Journal of Electrical and Electronics Research, 4(5), 294–299.

Patsakis, C., & Antoniou, G. (2019). "Security in *IoT* Networks: A Survey." IEEE Transactions on Network and Service Management, 16(2), 517-528.

Pradana, R.B.A. and Bhawiyuga, A. (2022) 'Pengembangan Platform *IoT Cloud* berbasis Layanan Komputasi *Server*less Google *Cloud* Platform (GCP)', Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer, 6(4 SE-), pp. 1841–1847.

Prastiyanto Dhidik (2012) 'Struktur Jaringan Komunikasi Data Paket Berdasar Protokol X.25', Teknik Elektro, 2(2), pp. 79–87.

Priantama, R. (2017) 'Efektivitas Wi-Fi dalam Menunjang Proses Pendidikan bagi Lembaga Perguruan Tinggi (Studi Kasus terhadap Mahasiswa Pengguna di Lingkungan Universitas

Kuningan)', Jurnal *Cloud* Information, 1(1), pp. 22–28.

Puspita, R. (2024) '*Internet of Things* (*IoT*) Menghubungkan Dunia Digital dan Fisik', Jurnal Teknologi Pintar, 4(2), pp. 1–20.

Rayes, A., & Salam, S. (2019). *Internet of Things* From Hype to Reality: The Road to Digitization. Springer.

Rittinghouse, J. W., & Ransome, J. F. (2016). *Cloud Computing*: Implementation, Management, and Security. CRC Press.

Schneider, E., Weik, M., & Klingert, S. (2016). Leveraging MQTT for *IoT* data collection. IEEE Sensors Journal, 16(13), 5385–5394.

Shelby, Z., Hartke, K., & Bormann, C. (2014). The Constrained Application Protocol (CoAP). IETF RFC 7252.

Sugiyatno, S., Sidiq, P. and Edrisy, I.F. (2024) 'Pengaruh Teknologi 5G pada Evolusi Komunikasi: Sebuah Kajian Terhadap Perkembangan dan Implikasinya di Bidang Sains', Nucleus, 4(2), pp. 115–120. Available at: https://doi.org/10.37010/nuc.v4i2.1448.

Syaikhu, A. (2013) 'Komputasi Awan Perpustakaan Pertanian', Jurnal Pustakawan Indonesia Volume 10 No. 1, 10(1), pp. 1–12.

Tan, F., Budiman, J.B. and Skynyrd (2023) 'Perbandingan Perkembangan Teknologi Berbasis Nirkabel di Daerah Pelosok dan Daerah Kota',

Jurnal Sains, Nalar, dan Aplikasi Teknologi Informasi, 2(2), pp. 25–31. Available at: https://doi.org/10.20885/snati.v2i2.23.

Tawalbeh, L. et al. (2020) '*IoT* Privacy and Security: Challenges and Solutions', Mdpi, pp. 1–17.

Tsiatsis, V., Karnouskos, S., Holler, J., Boyle, D., & Mulligan, C. (2018). "*Internet of Things*: Technologies and Applications for a New Age of Intelligence." Academic Press.

U.S. Department of Transportation (USDOT). (2018). Connected Vehicle Research Program.

Whitmore, A., Agarwal, A., & Da Xu, L. (2015). The *Internet of Things*—A Survey of Topics and Trends. Information Systems Frontiers, 17(2), 261–274.

Wibowo, A. (2021) Aplikasi Teknologi pada RFID pada *IoT*.

Wibowo, A. (2023) *Internet of Things* (*IoT*) dalam Ekonomi dan Bisnis Digital, Penerbit Yayasan Prima Agus Teknik. Available at: https://penerbit.stekom.ac.id/index.php/yayasanpat/article/download/436/461.

Wisnawa, I.P.O., Prasetia, I.P.W. and Lahallo, C.A.S. (2021) 'Arsitektur *Internet of Things* (*IoT*) Berskala Industri Dengan Fitur Auto Provisioning', TIERS Information Technology Journal, 2(2), pp. 24–30. Available at: https://doi.org/10.38043/tiers.v2i2.3312.

Wiwin Hartanto (2018) '*Cloud Computing* Dalam Pengembangan Sistem', Jurnal Pendidikan Ekonomi: Jurnal Ilmiah Ilmu Pendidikan, Ilmu Ekonomi dan Ilmu Sosial, 10(2), pp. 1–10.

World Bank. (2021). Digital Agriculture: A Review of the State of the Art.

Yang, Y., & Zhang, Y. (2021). "A Survey on Network Technologies and Applications for *Internet of Things* (*IoT*)." Computers, 10(7), 161.

Yusuf, M. et al. (2023) 'Penggunaan Teknologi *Internet of Things* (*IoT*) Dalam Pengelolaan Fasilitas Dan Infrastruktur Lembaga Pendidikan Islam', PROPHETIK Jurnal Kajian Keislaman, 1(2), pp. 1–18.

Zhang, Y., & Yang, L. (2020). "*Internet of Things* (*IoT*) Interoperability: The Key Challenges and Opportunities." Future Generation Computer Systems, 108, 528-540.

Zhou, W., Zhang, Y., & Liu, P. (2018). *Cloud*-assisted *IoT*-based sensor network security: Challenges and solutions. Future Generation Computer Systems, 76, 243–254.

INTERNET OF THING

IoT merupakan salah satu inovasi teknologi yang menghubungkan dunia digital dan fisik, memungkinkan perangkat-perangkat untuk saling berkomunikasi melalui jaringan internet. Dari sistem rumah pintar hingga aplikasi industri, IoT terus berkembang dan memberikan dampak signifikan dalam efisiensi, produktivitas, serta cara hidup manusia. Melalui buku ini, kami ingin memberikan pemahaman mendalam mengenai bagaimana IoT bekerja, potensi penerapannya, serta tantangan yang dihadapinya di masa mendatang.

Buku ini diharapkan dapat menjadi referensi yang berguna bagi mahasiswa, praktisi, dan siapa saja yang tertarik untuk memahami lebih jauh tentang IoT. Kami berusaha menyajikan materi dengan bahasa yang mudah dipahami namun tetap mengedepankan aspek teknis dan ilmiah agar pembaca dapat memperoleh gambaran yang jelas dan aplikatif.

IKAPI
IKATAN PENERBIT INDONESIA

CV REY MEDIA GRAFIKA
EMAIL:
REYMEDIAGRAFIKA.REM@GMAIL.COM

ISBN 978-623-8609-56-7
9 786238 609567