



**MODUL INTERNET OF THINGS (IoT)  
(PTI412)**

**MODUL SESI 3  
Ekosistem, Arsitektur dan Model Bisnis IoT**

**DISUSUN OLEH  
ADI WIDIANTONO, SKOM, MKOM.**

Universitas  
**Esa Unggul**

**UNIVERSITAS ESA UNGGUL  
2020**

# Ekosistem, Arsitektur dan Model Bisnis IoT

## 1. Kemampuan Akhir Yang Diharapkan

Setelah mempelajari modul ini, diharapkan mahasiswa mampu :

1. Memahami konsep Ekosistem IoT
2. Memahami Arsitektur dan Model Bisnis IoT.
3. Memahami penerapan dan tantangan IoT.

## 2. Uraian dan Contoh

### 1. Ekosistem IoT

#### 1.1. Pendahuluan

IoT diakui sebagai salah satu area terpenting dari teknologi masa depan dan mendapatkan banyak perhatian dari berbagai industri. IoT membawa perubahan paradigma yang secara radikal mengubah cara berbisnis dengan memungkinkan perusahaan mengembangkan layanan bernilai tambah dengan jaringan mesin dan perangkat mereka, meningkatkan layanan model bisnis mereka, dan meningkatkan keberlanjutannya. Misalnya, penyebaran sensor nirkabel di mana-mana meluas konektivitas digital ke fungsi, proses, dan operasi mesin dan layanan. Dengan menganalisis data yang dihasilkan oleh perangkat, perusahaan dapat menciptakan citra merek yang menguntungkan dan terlibat dalam komunikasi yang efektif.

Enterprise IoT, atau disebut juga IoT enterprise, mengacu pada semua perangkat terhubung yang digunakan untuk berbagai tujuan bisnis dalam pengaturan secara enterprise. Enterprise IoT adalah yang terbesar dari tiga sektor utama IoT - perusahaan, rumah, dan pemerintah. Sebagian besar perusahaan menyertakan inisiatif IoT enterprise di peta jalan strategis seperti meningkatkan operasi layanan, meningkatkan visibilitas ke dalam operasi, memungkinkan model bisnis baru, dan menciptakan penawaran produk dan layanan baru. Sementara perusahaan besar telah menjadi pengadopsi awal dan penerima manfaat dari inovasi IoT, semakin banyak usaha kecil dan menengah (UKM) juga memanfaatkan layanan IoT untuk

melayani pelanggan dengan lebih baik, meningkatkan produktivitas, memperluas basis pasar, dan tetap kompetitif.

Kebutuhan akan pengembangan aplikasi IoT yang efektif dalam kondisi yang realistis telah menghasilkan berbagai ekosistem metodologi dan platform IoT terintegrasi. Banyak perusahaan teknologi sedang mengembangkan berbagai platform IoT untuk membantu perusahaan dengan cepat mengembangkan dan menyebarkan layanan IoT untuk operasi dan peningkatan bisnis mereka. Platform ini menjadi sumber utama bagi perusahaan yang belum mempekerjakan insinyur yang mampu secara teknis dari berbagai bidang IoT. Platform IoT menyediakan fungsionalitas dasar dan alat pengembangan untuk berbagai aplikasi enterprise yang akan dikembangkan, tanpa upaya perancangan dan pemrograman yang mahal dan memakan waktu.

Tujuan Enterprise IoT adalah untuk menciptakan nilai tambah bagi organisasi bisnis dan pelanggan melalui layanan IoT. IoT platform baru terus muncul dan memberikan peluang dan tantangan potensial untuk IoT perusahaan. Untuk perusahaan, mengembangkan layanan IoT enterprise dengan berbagai platform yang disediakan oleh vendor seringkali lebih disukai daripada pengembangan secara in-house. Namun, ada kekurangan studi tentang ekosistem IoT dan arsitektur IoT yang berkaitan dengan pengembangan IoT enterprise. Misalnya, masih belum sepenuhnya memahami apa elemen ekosistem dan arsitektur IoT enterprise dan bagaimana memfasilitasi pengembangan layanan IoT enterprise tertentu. Mengingat kesenjangan dalam penelitian di sektor IoT enterprise.

## **1.2. Ekosistem IoT enterprise**

Suatu perusahaan tidak dipandang sebagai anggota dari industri tunggal tetapi sebagai bagian dari ekosistem bisnis yang melintasi berbagai industry [Moore]. Ekosistem umumnya dapat memiliki struktur bintang yang berpusat pada hub atau struktur datar seperti jala. Struktur bintang dapat ditemukan di Amerika Serikat di mana ekosistem IoT dibuat di sekitar perusahaan IT besar seperti Google, Amazon, Facebook, dan Apple yang berinteraksi dengan sejumlah besar perusahaan kecil, tetapi datar. Struktur ekosistem seperti jaring ditemukan di Eropa di mana ekosistem IoT terdiri dari perusahaan kecil dan gesit (*Agile*).

Ekosistem Enterprise membantu perusahaan bekerja secara kooperatif dan kompetitif di antara mereka sendiri untuk mendukung produk/layanan baru,

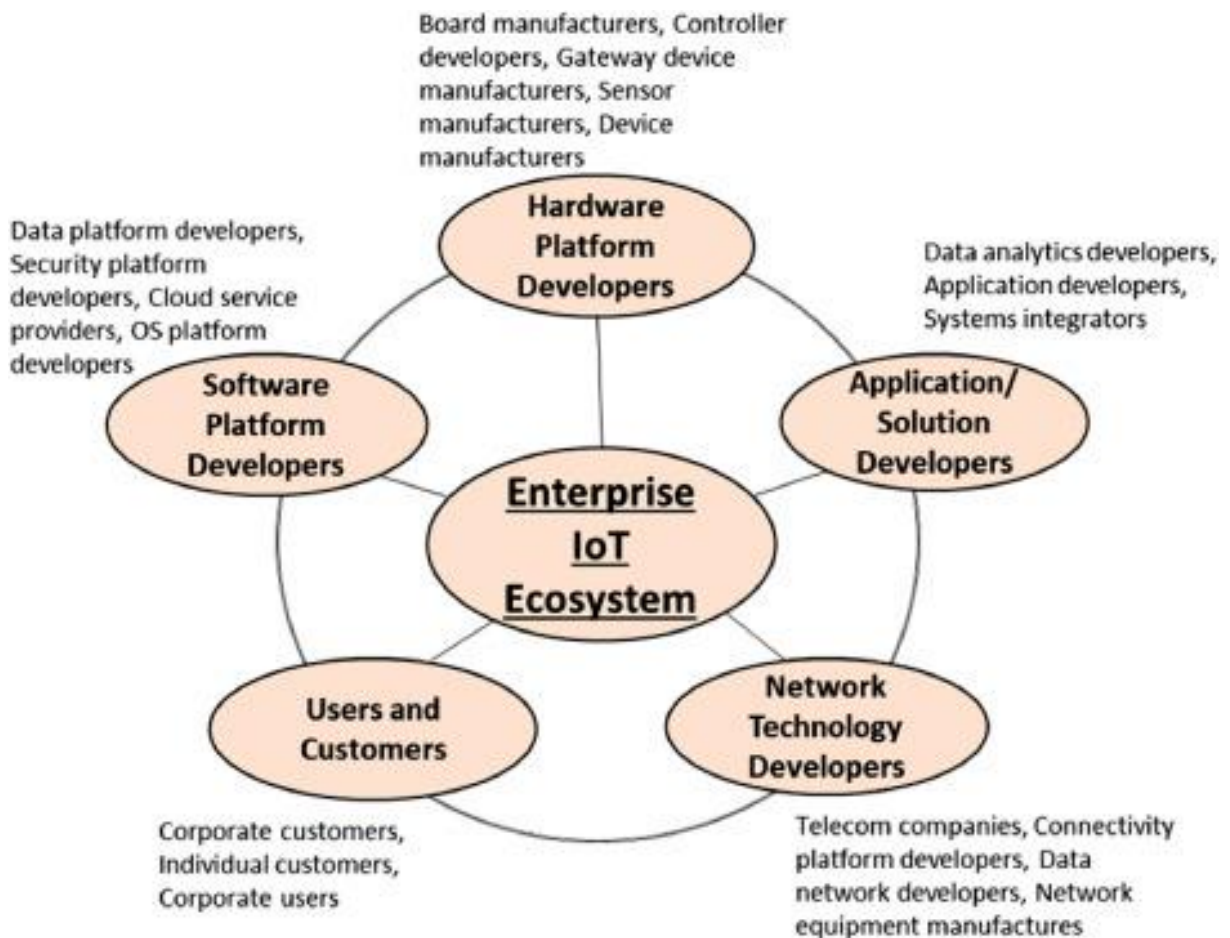
memperluas pasar, dan merangsang inovasi. Ekosistem bisnis IoT didefinisikan sebagai ekosistem jenis khusus dari ekosistem bisnis yang terdiri dari perusahaan dan individu terkait IoT yang berinteraksi bersama dengan lingkungan sosial ekonomi mereka [Mazhelis dkk]. Komunitas ekosistem IoT dapat terdiri dari penyedia platform perangkat lunak, penyedia platform perangkat keras, dan standarisasi. Dalam ekosistem IoT enterprise, pemangku kepentingan lintas industri dapat memberikan nilai tambah untuk ekosistem. Karena layanan IoT biasa memerlukan integrasi beberapa perangkat dan modul perangkat lunak yang sering dibuat oleh vendor yang berbeda, maka kebanyakan perusahaan tidak memiliki keahlian teknis yang dibutuhkan untuk mengembangkan layanan yang dibutuhkan. Pemahaman tentang ekosistem IoT enterprise akan membantu dalam memanfaatkan platform IoT yang tepat untuk pengembangan layanan. Misalnya, dalam manajemen rantai pasokan (SCM), perusahaan akan berusaha untuk memanfaatkan platform IoT terkait SCM untuk mengembangkan layanan IoT dengan cepat dan murah.

### **1.2.1. Pemain kunci ekosistem IoT enterprise**

Ekosistem IoT enterprise terdiri dari sejumlah besar pemangku kepentingan seperti penyedia platform, penyedia barang, pengembang, dan pengguna [16]. Berdasarkan survei praktik industri, lima pemain kunci Ekosistem IoT enterprise adalah:

- (1) pengembang platform perangkat lunak / *software platform developer* (misalnya, pengembang platform data, pengembang platform keamanan, penyedia layanan cloud),
- (2) pengembang platform perangkat keras / *hardware platform developer* (misalnya, produsen papan sirkuit, pengembang perangkat kendali, produsen perangkat gateway, produsen sensor, produsen perangkat),
- (3) pengembang teknologi jaringan / *network technology developer* (misalnya, perusahaan telekomunikasi, pengembang platform konektivitas, pengembang jaringan data),
- (4) pengembang aplikasi/solusi / *application/solution developer* (misalnya, pengembang analitik data, pengembang aplikasi, integrator sistem), dan
- (5) pengguna dan pelanggan / *user and costumer* (misalnya, pengguna korporat, pelanggan korporat, pelanggan individu).

Para pemain kunci ini secara simbiosis dan sinergis berkontribusi pada inovasi, memperluas pasar, memfasilitasi kolaborasi dan persaingan dalam industri, dan pada akhirnya menguntungkan perusahaan, pengguna, dan pelanggan.



Gambar 1. Pemain kunci ekosistem IoT enterprise

Komputasi awan memiliki kemampuan yang hampir tidak terbatas dalam hal penyimpanan dan kapasitas pemrosesan, melengkapi IoT, dan memecahkan beberapa masalah IoT. Platform IoT di cloud memainkan peran sebagai penerjemah dan distributor, menyimpan data dari berbagai perangkat dan mesin dan mengirimkannya melalui gateway ke layanan yang dipilih untuk diproses. Misalnya, infrastruktur IoT terintegrasi dengan platform cloud OpenStack untuk mengembangkan proyek kota pintar sehingga IoT dan infrastruktur kelas server dimanfaatkan, diabstraksikan, divirtualisasi, dan pada akhirnya diekspos secara homogen melalui API standar [Bruneoet at al]. Penyedia layanan cloud (CSP) seperti Microsoft, IBM, Amazon, dan Google memiliki kemampuan menurunkan hambatan teknologi untuk adopsi IoT perusahaan dengan menyederhanakan pengembangan aplikasi IoT dan menyediakan praktik terbaik dengan biaya lebih rendah. Tidak

seperti OS tradisional, OS untuk perangkat IoT harus memiliki desain yang ringan, sehingga memungkinkan ukuran kode rendah, kompleksitas rendah, dan konsumsi daya rendah. Misalnya, Google Brillo OS adalah versi Android ringan yang mendukung berbagai perangkat IoT dari berbagai produsen serta Wi-Fi, Bluetooth, dan perangkat protokol komunikasi berdaya rendah..

Banyak platform perangkat lunak IoT menyediakan layanan seperti kerangka kerja pemrograman, integrasi mesin-ke-mesin (M2M), manajemen data dan perangkat, keamanan dan penyimpanan, dan terjemahan protokol. Sejumlah peneliti menyarankan karakteristik dan fungsi yang diinginkan dari platform IoT.

Agar platform menarik bagi pengembang aplikasi, platform harus terbuka, berguna, mudah digunakan, dan mendukung API, platform perangkat lunak disarankan sbb:

- (1) menjadi dapat diprogram dengan bahasa pemrograman yang mudah,
- (2) menyediakan API tingkat tinggi untuk fungsi seperti sensor dan perangkat manajemen dan komunikasi,
- (3) mendukung eksekusi bersamaan dari beberapa aplikasi IoT dengan fungsi yang berbeda, dan
- (4) memungkinkan perangkat IoT pendamping untuk berkomunikasi dengan perangkat host-nya (misalnya ponsel cerdas Android) dan dapat dikontrol melalui perangkat host-nya [Lee dkk].

Yun dkk menyarankan bahwa platform perangkat lunak IoT mendukung portabilitas di berbagai perangkat keras dan sistem operasi, memberi pengembang lapisan abstraksi yang dapat menyembunyikan sistem dasar yang kompleks, dan memungkinkan akses transparan ke serangkaian API yang berguna untuk aplikasi.

### **1.2.2. Pengembang platform perangkat keras**

Platform perangkat keras yang kecil, mudah digunakan, dan murah telah berkontribusi pada perkembangan pesat IoT enterprise. Platform perangkat keras termasuk kit prototyping IoT dan papan siap pakai yang dibuat dengan mikrokontroler, prosesor, dan komponen lainnya. Platform ini memantau peristiwa fisik atau mungkin terhubung ke sistem yang lebih besar dengan tujuan: mengekstraksi data pemantauan. Beberapa papan platform IoT yang populer termasuk papan Espressif ESP8266, Raspberry Pi, Compute Module 3 (CM 3), Intel

Edison Compute Module, Adafruit Feather boards, Arduino IoT Product Line, Particle WiFi IoT hardware, dan littleBits. Platform perangkat keras IoT juga mencakup PC, tablet, smartphone, sensor, aktuator, dan perangkat periferal yang sering dibangun dari berbagai komponen. Persyaratan penting dalam merancang perangkat keras IoT platform adalah efisiensi energi yang dimungkinkan oleh miniaturisasi perangkat keras.

Banyak mikrokontroler IoT yang siap pakai dan komputer papan tunggal dirancang di sekitar IC system-on-a-chip (SoC) yang mengemas berbagai komponen ke dalam satu chip seperti unit pemrosesan pusat (CPU), memori, port input/output, penyimpanan sekunder, dan unit jaringan. Banyak perangkat IoT khusus berdasarkan papan komersial siap pakai dengan cepat mencapai batas kecepatan, konsumsi daya, dan ukuran perangkat. Untuk merancang perangkat IoT yang lebih efisien dengan chip yang terintegrasi, PCB yang lebih kecil, dan biaya keseluruhan yang lebih rendah per perangkat, pengembang sering mempertimbangkan platform berkinerja tinggi yang terdiri dari prosesor grafis atau implementasi fungsi tetap di field-programmable gate array (FPGA) atau aplikasi khusus implementasi sirkuit terintegrasi.

Sensor adalah perangkat keras penting lainnya untuk pengumpulan data dari lingkungan secara real time. Beberapa sensor IoT terhubung ke perangkat pengontrol IoT di mana peristiwa atau informasi tertentu memicu tindakan. Karena bertenaga baterai sensor memiliki umur energi yang terbatas, berbagai metode pemanenan energi telah dikembangkan (misalnya, penggunaan energi surya sel surya dan generator termoelektrik surya, energi mekanik, dan energi angin). Karena adanya tantangan/kesulitan dalam mengintegrasikan berbagai platform perangkat keras berpemilik (*proprietary hardware*) untuk pengembang yang tidak berpengalaman, maka platform perangkat keras sumber terbuka (*open source hardware*) mendapatkan popularitas cepat dalam pengembangan aplikasi IoT yang beragam dan baru.

### **1.2.3. Pengembang teknologi jaringan**

Operator telekomunikasi besar, pengembang platform konektivitas, pengembang jaringan data, dan produsen perangkat jaringan adalah *frontier* dari teknologi jaringan IoT seperti Bluetooth Low Energy (BLE), Zigbee, dan jaringan low-power wide-area (LPWA). Biasanya, komunikasi device-to-device (D2D) / machine to

machine (M2M) melibatkan komunikasi jarak pendek langsung antar perangkat tanpa dukungan infrastruktur jaringan. Salah satu platform komunikasi D2D paling populer untuk aplikasi perusahaan adalah Zigbee, yang merupakan jaringan nirkabel *ad-hoc* yang berdaya rendah, kecepatan data rendah, dan jarak dekat. Merupakan protokol komunikasi nirkabel jarak pendek berdasarkan spesifikasi berbasis IEEE 802.15.4, yang banyak digunakan dalam otomatisasi rumah dan industri di mana daya rendah diperlukan dan pertukaran data jarang dan rendah. Bluetooth, Radio Frequency Identification (RFID), dan Near Field Communication (NFC) juga banyak digunakan untuk konektivitas perangkat jarak dekat.

Di sisi lain, untuk wide area network untuk komunikasi IoT jarak jauh, teknologi low-power wide-area (LPWA) seperti NarrowBand-Internet of Things (NB-IoT), Long Term Evolution for Machines (LTE-M) , Sigfox, dan LoRa saat ini merupakan beberapa teknologi kunci. LPWA cocok untuk aplikasi IoT yang hanya perlu mengirimkan sejumlah kecil informasi dalam jarak jauh. NB-IoT adalah teknologi IoT seluler LPWA yang dikembangkan untuk menghubungkan berbagai perangkat IoT dan layanan dengan efisiensi spektrum dan jangkauan yang dalam. Sementara LoRa yang tidak berlisensi memiliki keunggulan dalam hal umur baterai, kapasitas, dan biaya, NB-IoT berlisensi menawarkan keunggulan dalam QoS, latensi, keandalan, dan jangkauan. Perlu dicatat bahwa tidak ada teknologi jaringan satu ukuran untuk semua ada karena aplikasi IoT yang berbeda memiliki persyaratan bisnis dan teknis yang berbeda dalam jaringan.

Jaringan generasi kelima (5G), generasi baru dalam teknologi seluler dan nirkabel, diluncurkan pada tahun 2020. Teknologi 5G dapat secara signifikan memperluas ranah aplikasi IoT dan akan memungkinkan IoT yang massif perangkat untuk berinteraksi satu sama lain dalam lingkungan baru. Ada antisipasi bahwa 5G akan memenuhi kebutuhan data kecepatan tinggi, latensi rendah, konsumsi energi hemat biaya, skalabilitas tinggi, konektivitas yang ditingkatkan, dan keamanan jaringan yang tinggi. 5G menyediakan tiga kategori layanan dengan persyaratan kinerja yang berbeda:

- broadband seluler yang ditingkatkan (enhanced Mobile Broad-Band /eMBB),
- komunikasi tipe mesin masif (massive Machine-Type Communication /mMTC), dan

- komunikasi latensi rendah yang sangat andal (Ultra-Reliable Low Latency Communication / UR-LLC) [37].

Namun, IoT berkemampuan 5G masih kekurangan dalam jaminan keamanan dan privasi yang memadai setelah jaringan logis dibagi dan komputasi kabut dibangun untuk layanan individu, yang mungkin dapat menghambat keberhasilan jaringan 5 G dan aplikasi IoT.

#### **1.2.4. Pengembang Aplikasi/Solusi**

Pengembang pihak ketiga, integrator sistem, dan pengembang internal sering menggunakan berbagai platform IoT untuk mengembangkan aplikasi/solusi khusus. Karena sifatnya yang kompleks dan terdistribusi, aplikasi/solusi IoT memakan waktu untuk berkembang, tidak dapat diandalkan, dan tidak mudah diskalakan. Selain itu, banyak profesional TI perusahaan tidak memiliki kemampuan teknis untuk mengembangkan solusi ujung ke ujung untuk perangkat yang saling berhubungan yang seringkali memerlukan middleware untuk integrasi antar perangkat. dan komunikasi. Untuk mengatasi tantangan ini, penting bagi pengembang dan insinyur untuk memanfaatkan platform untuk membangun, benchmark, dan mengoptimalkan aplikasi dan layanan. Pengembang memanfaatkan platform terbuka yang dapat dioperasikan dengan menyusun platform perangkat lunak dan perangkat keras IoT untuk berbagai layanan IoT. Misalnya, pengembang dapat memilih untuk mengintegrasikan Microsoft Azure IoT Starter Kit dengan Cisco Fog dan Intel Edison Compute Module untuk membuat solusi pemantauan jarak jauh.

Koeksistensi berbagai jenis perangkat, protokol, arsitektur, dan bahasa pemrograman membuat sistem IoT rumit untuk dikembangkan bahkan untuk pengembang berpengalaman karena kurangnya dokumentasi dari teknis dan perspektif konseptual. Oleh karena itu, integrator sistem adalah pemain penting dalam pengembangan aplikasi/solusi karena pengalaman mereka yang luas dalam mengintegrasikan solusi IoT di seluruh produsen dan industri. Perusahaan seringkali mencari saran dari sistem integrator untuk menemukan komponen arsitektur dan mengembangkan aplikasi untuk pengguna dan pelanggan.

#### **1.2.5. Pengguna dan pelanggan**

Perusahaan menyediakan layanan berbasis IoT kepada pengguna dan pelanggan untuk meningkatkan operasi bisnis dan layanan pelanggan mereka.

Pengguna dan pelanggan adalah penerima manfaat dan sumber pendapatan yang membuat inovasi IoT terus maju. Beberapa cara IoT mendukung pengguna dan pelanggan termasuk meningkatkan perawatan mesin, melacak kapal dan kendaraan, membantu pelanggan berbelanja, mendapatkan efisiensi dalam operasi checkout, dan mengelola keamanan dan utilitas kantor. Penerimaan layanan IoT oleh pengguna dan pelanggan sangat penting untuk investasi IoT untuk memenuhi potensi penuhnya. Baru baru ini studi menunjukkan bahwa manfaat yang dirasakan dan kenyamanan yang dirasakan dari layanan IoT secara positif mempengaruhi perilaku dalam menggunakan layanan IoT, tetapi risiko privasi yang dirasakan secara negatif mempengaruhi adopsi IoT.

### **1.3. Pemicu ekosistem IoT**

Ekosistem IoT telah berkembang dan berkembang dari waktu ke waktu. Pemicu memfasilitasi proses perubahan. Oleh karena itu, identifikasi dan pengelolaan faktor-faktor pendukung yang proaktif sangat penting untuk pertumbuhan ekosistem. Interoperabilitas dan keamanan/privasi diidentifikasi sebagai pendukung atau pemicu pengembangan ekosistem IoT.

#### **1.3.1. Interoperabilitas**

Menurut analisis McKinsey, ancaman substansial terhadap nilai ekonomi TI yang diprediksi adalah kurangnya interoperabilitas dan 40% dari potensi manfaat IoT dapat diwujudkan dengan interoperabilitas antara sistem IoT. Banyak IoT platform dan perangkat telah dikembangkan di masa lalu, tetapi sebagian besar platform dikembangkan dengan teknologi eksklusif. Platform berpemilik (proprietary) ini membuat sulit untuk memperluas sistem untuk mendukung layanan baru, mengintegrasikan data baru, dan beroperasi dengan sistem IoT lainnya. Beberapa pendekatan penanganan interoperabilitas yang diusulkan termasuk adapter/gateway, jaringan virtual/solusi berbasis overlay, jaringan yang ditentukan perangkat lunak (SDN), pendekatan berbasis IP, virtualisasi fungsi jaringan, API terbuka, arsitektur berorientasi layanan (SOA), teknologi web semantik, dan standar terbuka.

Salah satu pendekatan penanganan interoperabilitas yang menjanjikan adalah standarisasi. Fungsionalitas umum terstandarisasi memungkinkan perusahaan membuat aplikasi dan solusi yang dapat dioperasikan. Perusahaan IT terkemuka telah menciptakan berbagai aliansi industri untuk menetapkan standar dan

interoperabilitas perangkat. Aliansi industri yang disebut Thread Group (<http://www.threadgroup.org>). mengatasi tantangan interoperabilitas dengan menyediakan program sertifikasi yang memvalidasi kesesuaian perangkat dengan spesifikasi serta interoperabilitasnya terhadap jaringan campuran yang terdiri dari beberapa lapisan bersertifikat. Sekutu untuk Inovasi Internet of Things (AIOTI) diprakarsai oleh Komisi Eropa pada tahun 2015 dengan tujuan untuk menciptakan sebuah ekosistem IoT Eropa yang dinamis antara berbagai pemain IoT seperti perusahaan besar, UKM, dan perusahaan rintisan serta pusat penelitian, universitas, asosiasi, dan badan publik Eropa yang terkenal (<https://aioti.eu/>). Aliansi juga bertujuan untuk mendorong eksperimen, replikasi, dan penyebaran IoT dan mendukung konvergensi dan interoperabilitas standar IoT. OneM2M adalah kemitraan global yang dibentuk oleh delapan organisasi pengembangan standar (SDO) TIK untuk menstandarisasi Platform lapisan layanan M2M yang dapat dengan mudah disematkan dalam berbagai perangkat keras dan perangkat lunak, dan diandalkan untuk menghubungkan perangkat dengan server aplikasi M2M (<http://www.onem2m.org/>). Saat ini, ada hampir 200 anggota perusahaan dari semua sektor industri. spesifikasi oneM2M menyediakan kerangka kerja untuk mendukung aplikasi dan layanan seperti utilitas, transportasi, perawatan kesehatan, otomasi industri, rumah pintar, mobil terhubung, dan keselamatan publik.

Pemerintahan dalam suatu negara perlu menetapkan kebijakan dan peraturan tentang layanan yang mendukung IoT untuk mencapai ekonomi dan sosial sepenuhnya potensi. Pemerintah dan organisasi pembuat kebijakan lainnya dapat secara proaktif mendukung pengembangan interoperabilitas standar untuk perangkat dan sistem IoT. Mereka juga perlu menangani hak kekayaan intelektual dan lisensi untuk memfasilitasi adopsi standar oleh industri.

### **1.3.2. Security/Privacy**

Masalah keamanan dan privasi merupakan penghalang utama untuk adopsi layanan yang mendukung IoT. Keamanan dan privasi adalah segalanya yang lebih penting dalam konteks perusahaan. Bekerja dan tinggal di ruang yang dipenuhi dengan sensor dan kamera yang memantau setiap tindakan membuka peluang bagi penjahat dunia maya. Kurangnya keamanan dalam sistem IoT perusahaan juga dapat memberikan penyusup akses ke data sensitif pelanggan yang terkait dengan privasi dan transaksi bisnis. Kepercayaan dan adopsi layanan IoT bergantung pada

perlindungan keamanan/privasi yang mereka berikan. Seiring bertambahnya jumlah dan variasi yang terhubung perangkat diperkenalkan ke jaringan IoT, potensi ancaman keamanan tumbuh secara eksponensial. Beberapa aplikasi IoT digunakan untuk memantau infrastruktur keamanan tinggi seperti jaringan pintar dan fasilitas produksi bahan berbahaya lainnya. Aplikasi IoT mengumpulkan data pribadi yang sensitif seperti lokasi seseorang, kesehatan dan kebugaran, serta perilaku pembelian yang perusahaan ingin menganalisis. Potensi ancaman terhadap keamanan aplikasi ini dapat dikurangi dengan menetapkan protokol keamanan IoT seperti otentikasi, otorisasi, kontrol akses, dan non-penyangkalan dan menggabungkan keamanan mekanisme perlindungan seperti enkripsi data, firewall, dan analitik keamanan ke dalam sistem IoT.

Memasukkan persyaratan privasi pada tahap awal pengembangan IoT sangat penting untuk menciptakan kecukupan kepercayaan publik dan memfasilitasi adopsi sistem IoT. Banyak perangkat IoT yang hemat energi dan ringan. Perangkat ini mencurahkan sebagian besar energi yang tersedia dan sumber daya komputasi untuk mendukung fungsi inti, membuat tugas, mendukung keamanan dan privasi cukup menantang. IoT dapat memanfaatkan blockchain dalam mengamankan banyak aplikasi berorientasi IoT dengan menerbitkan dan menyimpan data sebagai buku besar publik yang tidak dapat diubah karena setiap pengguna atau node dalam sistem mempertahankan buku besar yang sama dengan semua pengguna atau node lain dalam jaringan. Blockchain memberikan keamanan dan privasi terdesentralisasi, tetapi melibatkan energi, penundaan, dan overhead komputasi yang signifikan yang belum sesuai untuk sebagian besar sumber daya yang terbatas pada perangkat IoT. Sementara blockchain kemungkinan akan memainkan peran penting dalam keamanan IoT, tantangan teknis ini harus diatasi sebelum adopsi luas blockchain di IoT terjadi.

Pemerintah dapat memainkan peran penting dalam mengatasi masalah keamanan terkait penggunaan layanan IoT. Di AS, mulai Juli 2018, tiga RUU yang tertunda diusulkan [55]. Cyber Shield Act 2017 (S. 2020, 115 Cong. (2017)) adalah RUU sukarela di mana produsen perangkat IoT mematuhi protokol keamanan IoT tertentu dan sebagai imbalannya diberikan sertifikasi pemerintah bahwa perangkat mereka aman. RUU sukarela lainnya, Internet of Medical Things Resilience Partnership Act of 2017 (the Medical Things Act) (H.R. 3985, 115 Cong. (2017)), akan membentuk kelompok kerja entitas publik dan swasta yang dipimpin oleh Food

and Drug Administration (FDA) untuk merekomendasikan kerangka kerja sukarela dan pedoman untuk keamanan dan ketahanan perangkat Internet of Medical Things. Undang-Undang Peningkatan Keamanan Siber akan mengharuskan vendor perangkat IoT untuk memenuhi kriteria tertentu sebelum lembaga pemerintah AS dapat membeli perangkat. Undang-undang mengharuskan perangkat IoT: dapat ditambah, tidak mengandung kerentanan yang diketahui, bergantung pada protokol standar, dan tidak mengandung kata sandi yang dikodekan secara *hard-code*.



## 2. Arsitektur Ekosistem IoT Enterprise

Tidak ada konsensus tunggal tentang arsitektur untuk IoT, yang disepakati secara universal. Arsitektur yang berbeda telah diusulkan oleh peneliti yang berbeda. Tidak ada arsitektur standar untuk ekosistem IoT. Aspek dalam arsitektur IoT merupakan bidang penelitian yang dipelajari secara aktif. Arsitektur IoT yang terstruktur dengan baik akan membantu perusahaan menciptakan inovasi. Ekosistem IoT enterprise yang dibahas di bagian sebelumnya menyediakan platform teknologi yang diperlukan untuk implementasi arsitektur IoT. Meskipun tidak ada arsitektur IoT yang disepakati di antara para peneliti, umumnya menggunakan pendekatan berlapis-lapis, dengan setiap lapisan didedikasikan untuk fungsi-fungsi tertentu seperti komunikasi/penginderaan, pengolahan data, dan pengolahan/penalaran pengetahuan. Untuk pengembangan layanan IoT yang sukses, arsitektur IoT perlu: diciptakan dan diperbarui terus-menerus untuk menugaskan dan menonaktifkan berbagai aset dan layanan IoT.

### 2.1. Arsitektur Tiga Lapis

Arsitektur Tiga Lapis, merupakan arsitektur yang paling dasar, dan diperkenalkan pada tahap awal penelitian di bidang ini. Memiliki tiga lapisan, yaitu persepsi, jaringan, dan lapisan aplikasi.

**(i) Lapisan persepsi (*perception layer*)**, adalah lapisan fisik, yang memiliki sensor untuk merasakan dan mengumpulkan informasi tentang lingkungan. Ia merasakan beberapa parameter fisik atau mengidentifikasi objek pintar lainnya di lingkungan. Lapisan persepsi ini untuk pengumpulan data. Lapisan persepsi memainkan peran penginderaan untuk sistem IoT back-end, dikenal juga sebagai lapisan sensor. Persepsi lapisan terdiri dari perangkat yang berbeda seperti sensor, tag dan pembaca RFID, kamera video, dan ponsel pintar yang digunakan untuk mengidentifikasi objek dan lokasi serta mengumpulkan data dari lingkungan sekitar. Lapisan persepsi sering menghasilkan sejumlah besar data yang perlu dikumpulkan dan dianalisis untuk menanggapi berbagai peristiwa secara real time.

**(ii) Lapisan jaringan (*network layer*)**, bertanggung jawab untuk menghubungkan ke *smart things* lainnya, perangkat jaringan, dan server. Fiturnya juga digunakan untuk transmisi dan pemrosesan data sensor. Lapisan jaringan, juga dikenal sebagai

lapisan transmisi/*transport*, mentransmisikan data yang dikumpulkan dari sensor ke lapisan berikutnya melalui berbagai jaringan. Ini bertindak sebagai jembatan antara lapisan persepsi dan lapisan aplikasi. Lapisan ini menyediakan infrastruktur untuk mendukung koneksi nirkabel atau kabel antar perangkat. Lapisan jaringan menggunakan gateway Internet, switching, dan perangkat perutean bersama dengan teknologi komunikasi seperti WiFi, LTE, Bluetooth, 3G, dan Zigbee. Penyebaran, manajemen, dan penjadwalan jaringan sangat penting untuk lapisan jaringan.

**(iii) Lapisan aplikasi (*Application Layer*)**, bertanggung jawab untuk mengantarkan layanan tertentu dari aplikasi kepada pengguna, yang disediakan oleh berbagai aplikasi di mana IoT dapat digunakan, misalnya, rumah pintar, kota pintar, dan kesehatan yang cerdas. Lapisan aplikasi lebih ke pengenalan/pengakuan objek dan hubungan antar-objek. Lapisan aplikasi terdiri dari sekumpulan aplikasi/solusi khusus masalah yang berinteraksi dengan pengguna, memecahkan masalah, dan berbagi masalah dan solusi dengan aplikasi lain. Lapisan aplikasi juga bertanggung jawab untuk mengintegrasikan data dan informasi dan menyajikannya kepada pengguna dalam format yang ramah pengguna. Pada lapisan aplikasi, persyaratan utama seperti: akurasi, efisiensi energi, dan latensi rendah dapat bervariasi tergantung pada jenis/sektor aplikasi IoT dikembangkan. Untuk memfasilitasi pengembangan aplikasi dengan perangkat heterogen pada lapisan aplikasi, sejumlah aplikasi menggunakan protokol lapisan, yang diantaranya, Constraint Application Protocol (CoAP) atau Message Queue Telemetry Transport (MQTT).

Arsitektur tiga lapis mendefinisikan ide utama dari IoT, tetapi itu tidak cukup untuk penelitian/pengembangan tentang IoT karena penelitian sering berfokus pada aspek lainnya dari IoT yang lebih luas/dalam.

## **2.2. Arsitektur lima lapis**

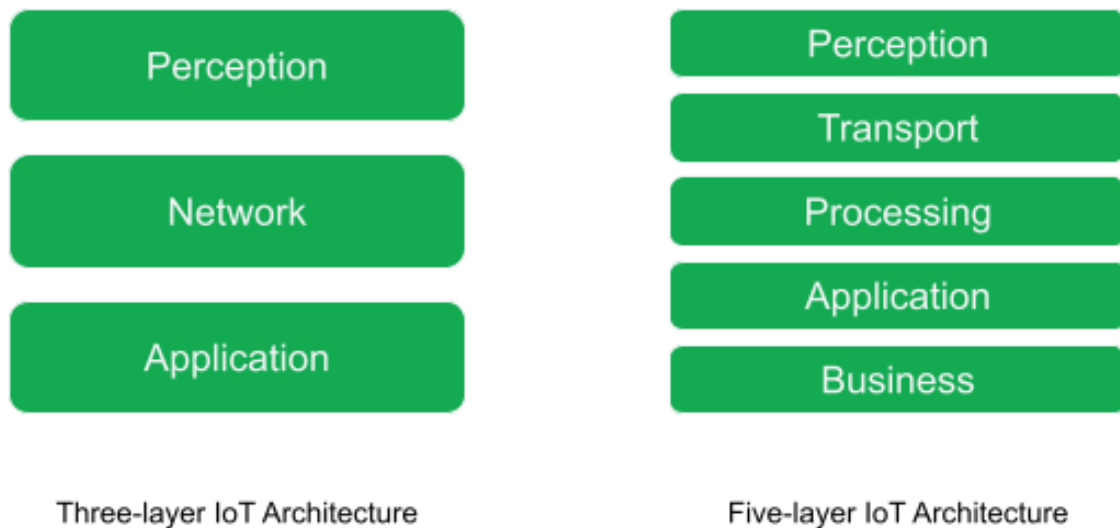
Dengan kemajuan dalam IoT, para peneliti mengusulkan empat lapisan dan arsitektur lima lapis. Arsitektur lima lapisan menambahkan lapisan pemrosesan dan lapisan bisnis di atas arsitektur tiga lapis. Selain itu lapisan jaringan (*network layer*) di berikan nama sebagai lapisan transmisi (*transport layer*). Berikut lapisan yang ditambahkan di arsitektur lima lapis:

**(iv) Lapisan pemrosesan (*Processing Layer*)**, juga disebut lapisan middleware, membersihkan, menyimpan, menganalisis, dan memproses data yang diangkut dari lapisan jaringan. Lapisan pemrosesan berisi platform seperti manajemen basis data, analitik data, dan cloud komputasi. Karena data besar yang dihasilkan dari perangkat IoT, banyak aplikasi IoT memerlukan penyimpanan data yang sangat besar, sangat besar kecepatan pemrosesan untuk memungkinkan pengambilan keputusan waktu nyata, dan jaringan broadband berkecepatan tinggi untuk mengalirkan data, audio, atau video. Komputasi awan menjadi teknologi yang cocok untuk menangani aliran data yang sangat besar dan memprosesnya untuk sejumlah besar perangkat IoT secara real time. Infrastruktur terdistribusi yang kompleks dari IoT membutuhkan penyederhanaan pengembangan aplikasi dan solusi baru. Lapisan pemrosesan dapat menyembunyikan detail platform dan ideal untuk pengembangan aplikasi IoT.

**(v) Lapisan bisnis (*Business Layer*)**, Lapisan paling atas arsitektur IoT enterprise adalah lapisan bisnis, mengelola seluruh sistem IoT, termasuk aplikasi, model bisnis dan keuntungannya, dan privasi pengguna. Disebut juga sebagai **lapisan manajemen layanan (*Service Management Layer*)** yang bertanggung jawab atas pemilihan dan pengiriman layanan IoT perusahaan. Lapisan manajemen layanan adalah titik awal untuk mengembangkan satu set layanan IoT enterprise. Manajemen layanan dalam hal ini mengacu pada kegiatan dan prosedur pendukung yang dilakukan oleh organisasi untuk merencanakan, merancang, mengimplementasikan, mengoperasikan, dan meningkatkan layanan IoT perusahaan yang digunakan oleh pelanggan.

Layanan IoT mengacu pada aktivitas yang dilakukan untuk menciptakan nilai bagi pengguna dan pelanggan melalui penggunaan aplikasi/solusi. Layanan IoT khusus domain apa pun harus mendukung strategi perusahaan tingkat tinggi. Layanan IoT menciptakan nilai bagi pengguna dan pelanggan yang dapat diukur dengan kesiediaan pengguna untuk membayar dan menggunakan kembali layanan.

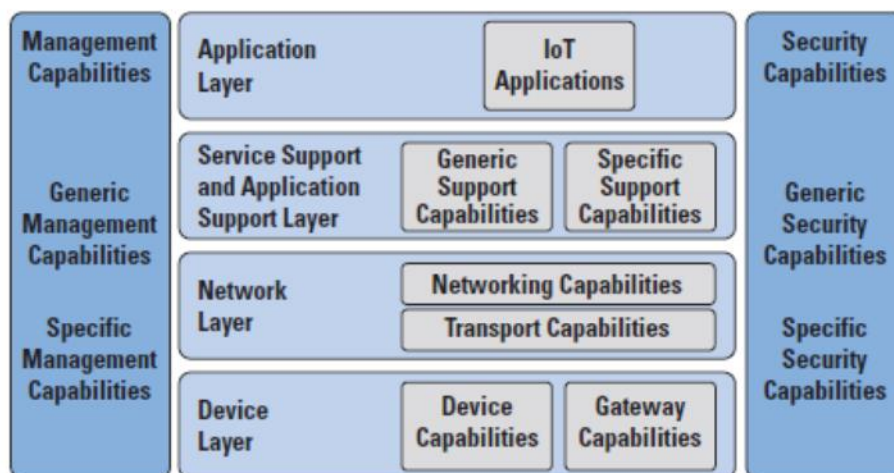
Lapisan manajemen layanan memberikan arahan untuk empat lapisan tingkat yang lebih rendah. Elemen kunci dari lapisan manajemen layanan adalah model bisnis layanan IoT.



Gambar 2. Arsitektur IoT

### 2.3. Arsitektur Referensi IoT

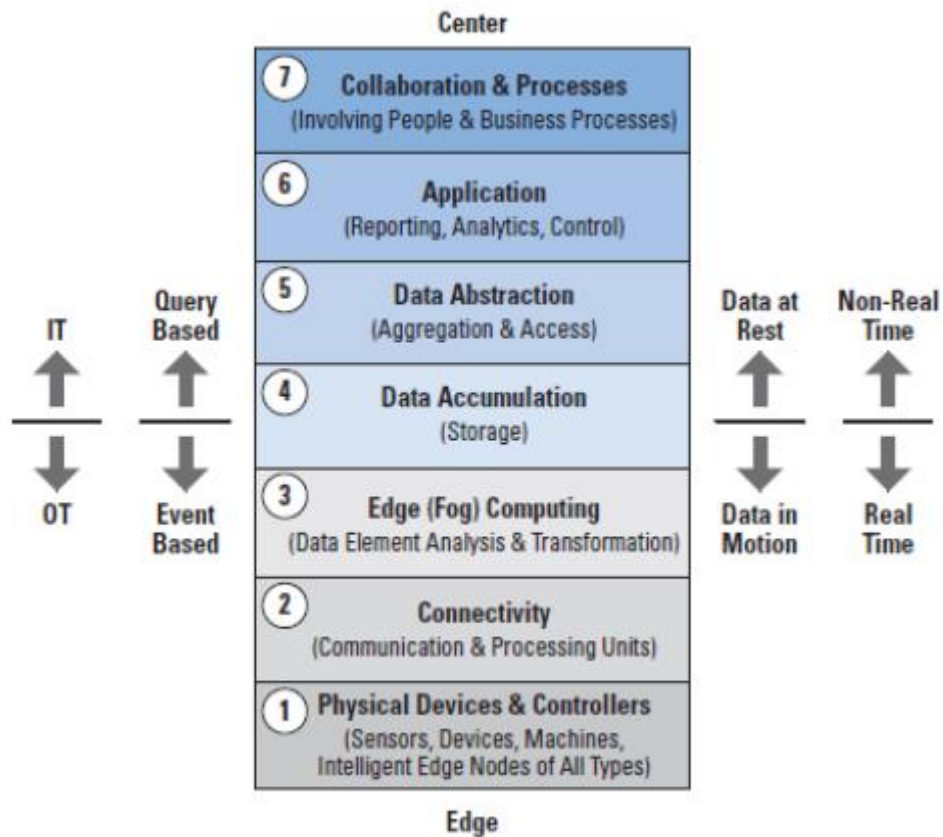
Beberapa organisasi mendefinisikan dan menyediakan Arsitektur IoT sebagai model referensi, salah satunya adalah ITU-T (*International Telecommunication Union – Telecommunication*) yang merupakan kelompok studi standarisasi bidang telekomunikasi. ITU-T mengilustrasikan Arsitektur IoT dengan arsitektur berlapis seperti pada gambar 3.



Gambar 3. Model Referensi Arsitektur ITU-T IoT (Recommendation Y.2060)

Model Referensi Arsitektur IoT dari ITU-T mengadopsi Arsitektur empat lapisan dengan ditambahkan dengan Kemampuan Pengelolaan (*Management Capabilities*) dan Keamanan (*Security Capabilities*).

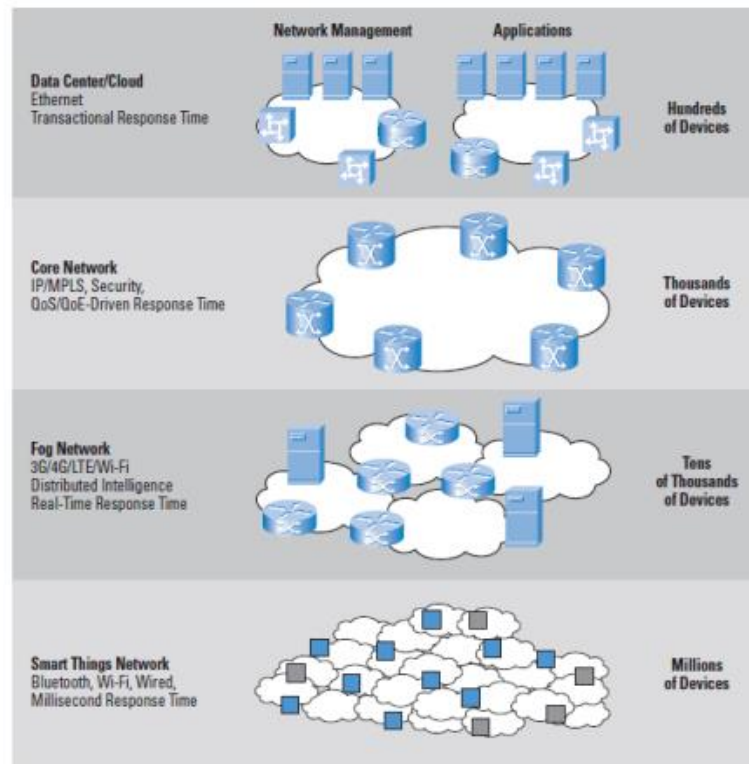
Selanjutnya ada *IoT World Forum (IWF)* yang juga merilis Model Referensi untuk Arsitektur IoT. Arsitektur ini mengakomodasi teknologi cloud/fog yang digunakan untuk membangun Enterprise IoT.



Gambar 4. Model Referensi Arsitektur IoT IWF.

EDGE/FOG COMPUTING digunakan dalam:

- Penerapan IoT, data dalam jumlah besar dihasilkan oleh sensor-sensor dalam jaringan terdistribusi.
- Memproses data sedekat mungkin dengan sensor lebih dibutuhkan, daripada menyimpan seluruh data dalam pusat penyimpanan data,
- Tujuan dari level edge computing adalah untuk mengubah aliran data menjadi informasi yang cocok untuk disimpan dan diproses di tingkat yang lebih tinggi.
- Contoh operasi : evaluasi, memformat ulang data, dan merangkum atau mengurangi data
- Edge computing, disebut . juga fog computing, adalah karakteristik pembeda IoT dengan teknologi lainnya. Istilah fog (kabut) terinspirasi dari fakta bahwa kabut cenderung melayang rendah mendekati tanah, sedangkan cloud (awan) berada di atas langit yang tinggi.



Gambar 5. Edge/Fog Computing

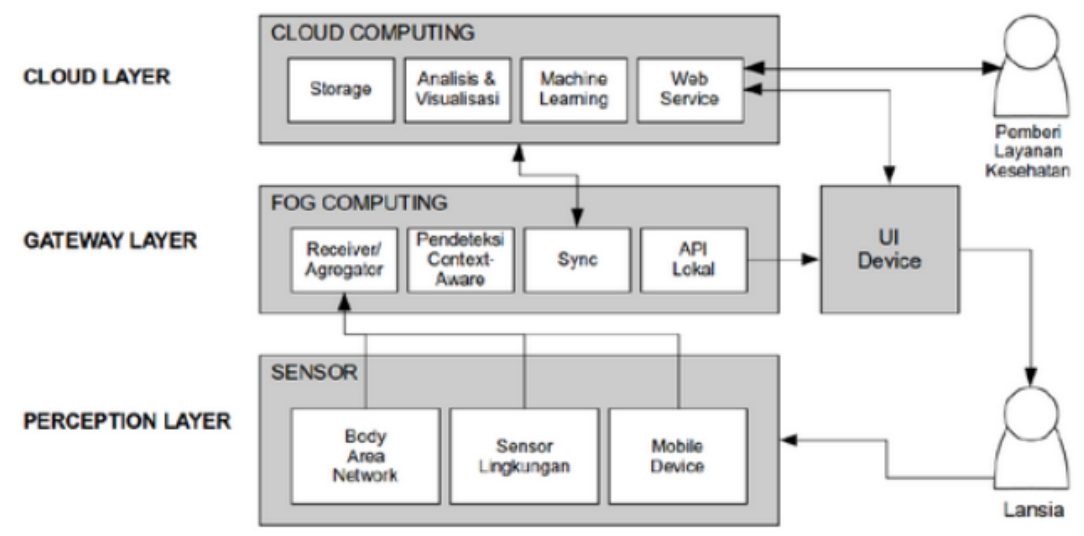
### Perbandingan Edge dan Cloud

	Cloud	Fog
<b>Location of processing/ storage resources</b>	Center	Edge
<b>Latency</b>	Low to high	Low
<b>Access</b>	Fixed or wireless	Mainly wireless
<b>Support for mobility</b>	Not applicable	Yes
<b>Control</b>	Centralized/hierarchical (full control)	Distributed/hierarchical (partial control)
<b>Service access</b>	Through core	At the edge/on handheld device
<b>Availability</b>	99.99%	Highly volatile/highly redundant
<b>Number of users/devices</b>	Tens/hundreds of millions	Tens of billions
<b>Main content generator</b>	Humans and devices	Devices/sensors
<b>Content generation</b>	Central location	Anywhere
<b>Content consumption</b>	End device	Anywhere
<b>Software virtual infrastructure</b>	Central enterprise servers	User devices

## 2.4. Penerapan Arsitektur IoT

Berikut ini beberapa gambaran/ilustrasi pemanfaatan Arsitektur IoT untuk Model Bisnis tertentu.

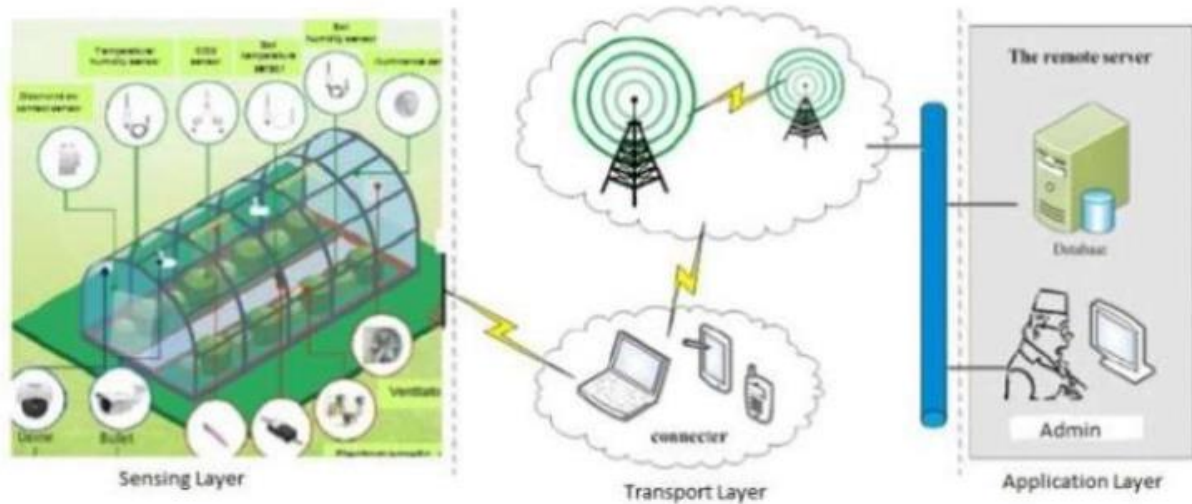
- Tele-HomeCare



Sumber : PERANCANGAN ARSITEKTUR TELE-HOMECARE BERBASIS INTERNET OF THINGS DENGAN CONTEXT-AWARE DAN FOG COMPUTING, Trie Maya Kadarina, Rinto Priambodo, SIMNAS RISTEK, 2019

Gambar 6. Arsitektur IoT Tele-HomeCare

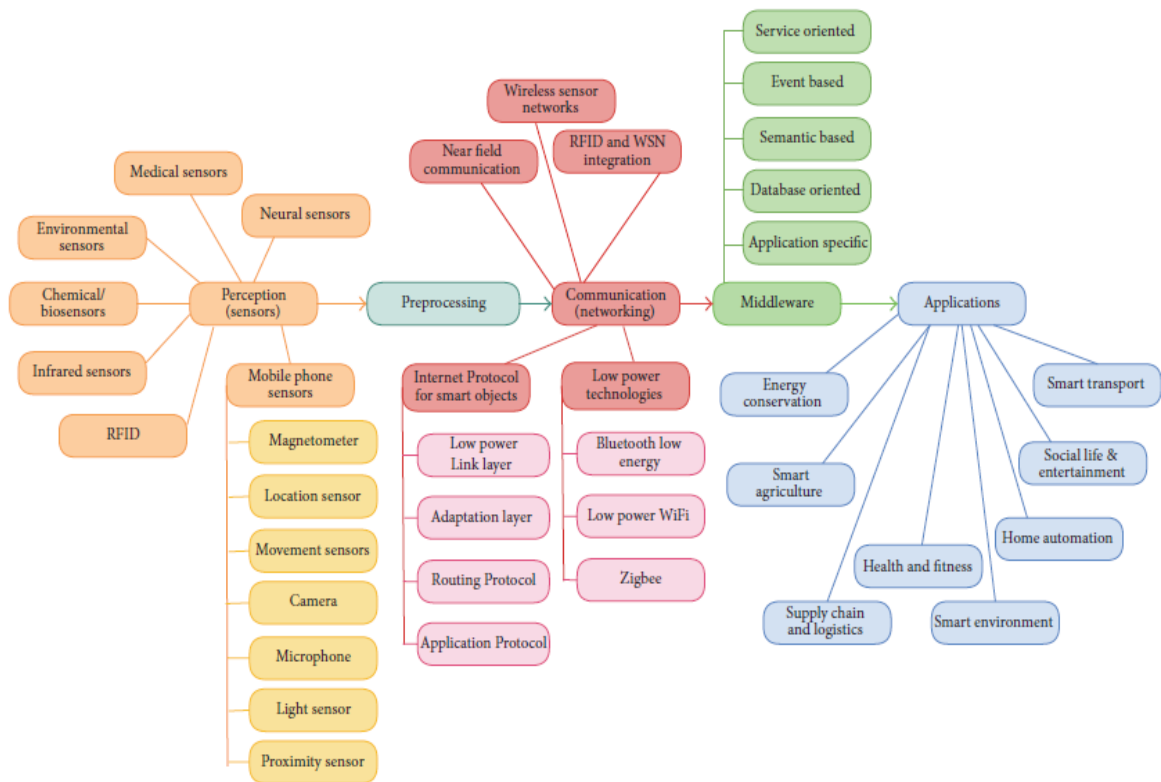
- Agroindustri



Gambar 7. Arsitektur IoT Agroindustri

### 3. Taksonomi riset pengembangan Teknologi IoT

Berdasarkan Arsitektur IoT yang telah dibahas sebelumnya, berikut ini gambaran taksonomi dari riset pengembangan teknologi IoT.



Gambar 8. : Taxonomy of research in IoT technologies.

### C. Daftar Pustaka

Pethuru Raj, Anupama C. Raman, *The Internet of Things : Enabling Technologies, Platforms, and Use Cases*, Ch 1, CRC Press, Taylor and Francis Group, 2017

