**ITEJ Juli-2019, Volume 4 Nomor 1 Page 39 - 51**

**ITEJ**
Information Technology Engineering Journals
eISSN : 2548-2157

Url : https://syekhnurjati.ac.id/journal/index.php/itej
Email : itej@syekhnurjati.ac.id

# Future of Internet of Things in Smart City

Erni Dianawati
*Sekolah Teknik Elektro dan Informatika*
*Institut Teknologi Bandung*
Bandung, Indonesia
ernidianawatiw@students.itb.ac.id

***Abstract*— internet of things has become a scientific field that continues to grow from time to time. unconsciously humans have relied heavily on the use of devices - IoT devices in their daily lives. in its development IoT has also become one of the technologies that plays a big role in the development of Smart City in the world. still many. in this paper we will discuss a number of issues that may arise in implementing IoT in Smart City and some of the solutions that have been reviewed.**

***Keywords—Internet of Things(IoT), Smart City***

## I. PENDAHULUAN

Internet of Things didefinisikan sebagai sebuah teknologi yang memungkinkan manusia dan *things*(alat) saling berhubungan kapan saja, dimana saja, dengan apa saja dan siapa saja dengan memanfaatkan jaringan dan layanan apa saja[1]. Visi utama dari IoT adalah untuk membentuk lingkungan yang cerdas dengan memanfaatkan berbagai benda/perangkat pintar yang memiliki kemampuan sensorik dan berkomunikasi untuk menghasilkan data dan mengirimkannya melalui jaringan internet untuk pengambilan keputusan. Keputusan tersebut digunakan untuk mengatasi berbagai macam masalah yang berkaitan dengan kegiatan manusia sehari-hari.

Semakin banyaknya penggunaan IoT dalam layanan pintar dan aplikasi saling berkelanjutan melalui proses pengambilan keputusan, maka penggunaan layanan pintar ini banyak memanfaatkan konsep dari teknologi lain seperti aplikasi, algoritma, pengembangan perangkat lunak, komputasi seluler, otomatisasi melalui kecerdasan buatan, pembelajaran mesin dan layanan berbasis lokasi. Layanan cerdas dan aplikasi yang dimaksud termasuk Smart City, Smart Grid, Smart Transport, Smart Health, Smart Home, dan aplikasi – aplikasi cerdas lainnya. [ 2 ]

Dalam beberapa penelitian perangkat yang terhubung dengan IoT pada masa mendatang diperkirakan bisa mencapai 100 miliar alat seiring dengan perkembangan penggunaan IoT dalam kehidupan sehari-hari, yang mengakibatkan manusia dan hal-hal lain disekitarnya saling terhubung melalui internet. Kondisi tersebut menjadikan keamanan dan privasi serta penggunaan energi merupakan tantangan yang cukup besar alam IoT untuk menciptakan sebuah ekosistem IoT yang terpercaya dan hemat energi seiring dengan semakin besar dan banyaknya pertukaran data antar perangkat yang terhubung di internet.

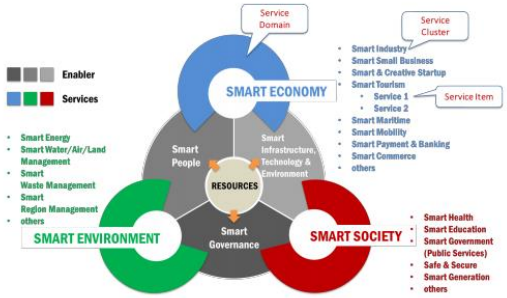
## II. INTERNET OF THINGS(IOT) DALAM SMART CITY

IoT didefinisikan sebagai enabler teknolohi untuk pengembangan lingkungan yang cerdas di masa depan. Hal ini banyak mendorong transformasi digital dari berbagai lingkungan yang beebeda-beda (transportasi, lingkungan, industry, kesehatan dan lain-lain) yang banyak digunakan pada kehidupan sehari-hari. [3]

IoT menyediakan individu, masyarakat dan dunia bisnis sebuah peluang baru untuk mengakses data untuk dikembangkan menjadi aplikasi dan layanan baru untuk menciptakan lingkungan yang lebih bersih dan masyarakat yang lebih cerdas. Informasi menjadi pilar utama bagi perencanaan kota, arsitek, pengembang, penyedia transportasi serta dalam penyediaan layanan publik.[4]

Menurut Eckhoff dkk(2018), sebuah kota dapat disebut Kota Cerdas ketika adanya investasi pada manusia dan social dengan tradisional(seperti transportasi) dan infrastruktur komunikasi yang modern (ICT) yang dapat memicu pertumbuhan ekonomi yang berkelanjutan dan kualitas hidup yang tinggi, dengan pengelolaan Sumber Daya Alam secara bijaksana melalui partisipasi Pemerintah.

Model Kota Cerdas dalam Garuda Smart City Framework(GSCF) digambarkan dengan melihat hubungan pada 3 lapisan yaitu Lapisan Sumber daya, lapisan enabler dan lapisan layanan seperti digambarkan pada gambar dibawah. [5]



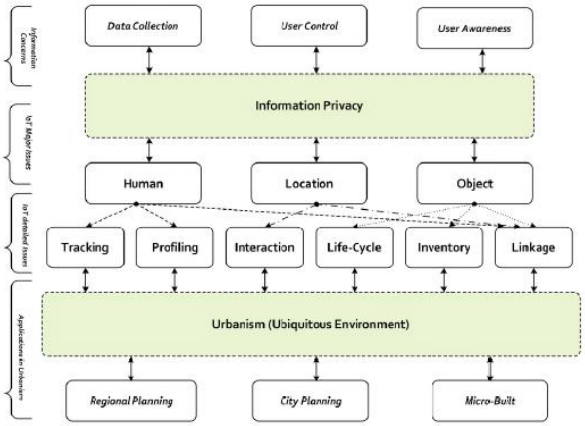

Gambar. 1 Garuda Smart City Framework(GSCF) [5]

Inovasi-inovasi yang dikembangkan untuk Kota Cerdas bukan berfokus pada aplikasi apa saja, tetapi dalam penggunaan teknologi yang mendasarinya. Dalam penelitiann tersebut, tekologi yang biasa digunakan dapat dikelompokkan menjadi Sembilan kategori yaitu ubiquitous connectivity, smart card, wearable devices, Internet of Things(IoT), intelligent vehicles, autonomous systems, cloud computing dan open data. Sebagian besar aplikasi yang diterapkan pada Kota Cerdas bergantung pada beberapa kombinasi dua atau lebih dari teknologi yang memungkinkan. Misalnya kombinasi dari jaringan IoT dengan ubiquitous connectivity yang memungkinkan pemantauan lalu lintas maupun polusi udara secara real-time di seluruh kota. [4]

## III. TANTANGAN DALAM PENGEMBANGAN IOT

### *A. Privasi*

Salah satu peran IoT adalah untuk meningkatkan peralatan yang ada dengan menggunakan kemampuan penginderaan(sensing) dan komunikasi untuk mengumpulkan data, hal ini memungkinkan penyedia layanan dan pihak yang terlibat untuk mempelajari informasi – informasi sensitive tentang objek[4]. IoT juga memfasilitasi pertukaran informasi antar objek yang saling terhubung, sehingga memungkinkan banyaknya data individu/personal dan hal-hal lain yang didapat dari perangkat cerdas yang terkumpul. Meskipun pada perangkat yang terhubung biasanya akan ada dokumen persetujuan pengguna mengenai pengumpulan informasi, tetapi kebanyakan pengguna tidak membaca dokumen tersebut sampai akhir. Hal ini memungkinkan adanya penyalahgunaan informasi tanpa sepengatahuan atau persetujuan pengguna[6]




Gambar 2. keterhubungann informasi data dengan lingkungan [7]

Ancaman privasi di IoT dapat dikelompokkan kedalam 6 kategori yaitu identifikasi dan pelacakan individu, profil pengguna, interaksi dan presentasi, transisi siklus hidup, serangan inventaris dan *linkage* seperti tergambar pada gambar diatas. Selain itu, masalah privasi pada teknologi IoT juga termasuk masalah terkait privasi manusia, privasi lokasi dan privasi objek(thing). Paradigma IoT mencakup pembangunan infrastruktur cerdas di seluruh kota dengan sejumlah banyak perangkat, sensor dan koneksi. Besarnya biaya tambahan yang harus dikeluarkan untuk mengamankan perangkat IoT dan koneksi antar keduanya, membuat asumsi jika hanya negara – negara kaya saja yang dapat menerapkan jaringan IoT.

Sedangkan dalam penelitian lain disebutkan jika resiko privasi dapat dikategorikan menjadi 5 jenis yang bisa saja muncul ketika pengimplementasiaannya di berbagai aplikasi dan teknologi kota cerdas. [4]

1) Privasi lokasi : informasi ini tidak hanya termasuk lokasi itu sendiri tetapi juga kapan dan berapa lama pengguna mengunjungi lokasi tersebut. Misalnya pelanggaran privasi lokasi dapat menyebarluaskan rumah ataupun tempat kerja pengguna, pola berbelanja dimana, dan lain – lain.
2) Privasi keadaan tubuh dan pikiran : keadaan tubuh dan pikiran yang dimaksud meliputi karakteristik tubuh seseorang termasuk biometric, kesehatan, genom, keadaan mental, emosi dan pemikiran. Pelanggaran privasi ini dapat mempengaruhi diskriminasi oleh penyedia dan perusahaan asuransi.
3) Privasi dalam kehidupan soaial: kehidupan social seseorang termasuk interaksi sosial seperti apa yang dikatakan dalam percakapan atau apa yang diposting di platform media sosial. Privasi ini juga termasuk metadata tentang interaksi tersebut seperti berinteraksi dengan siapa, kapan dan untuk berapa lama. Pelanggaran dalam privasi ini memungkinkan diketahuihya interaksi dengan rumah sakit sampai infoormasi politik maupun pendapat seseorang.
4) Privasi perilaku dan tindakan seseorang mencakup kebiasan, hobi, tindakan dan pola pembelian. Misalnya penyebaran detail informasi ketika melakukan belanja online saat menggunakan katu kredit saat transaksi.
5) Privasi media: privasi ini mencakup privasi gambar, video, audio dan data lainnya. Privasi ini bisa termasuk rekaman CCTV(dalam keadaan sadar maupun tidak sadar, selain itu rekaman kamera atau media yang diunggah ke internet. Mendistridusikan ulang atau menyebarkan informasi media tanpa persetujuan pihak yang terkait merupakan contoh pelanggaran terhadap privasi ini.

### *B. Keamanan*

Isu keamanan dalam perangkat IoT sering diabaikan dalam proses pengembangan perangkat dan teknologi IoT, hal ini banyak dikarenakan waktu pengmbangan yang singkat dan juga pengurangan biaya dalam proses desain dan pengembangan perangkat. Hanya sedikit perangkat yang terlindungi,

biasanya hanya fokous terhadap perlindungan perangkat lunak tanpa terlalu berfokus pada perlindungan perangkat keras, seperti autentifikasi firmware. [8]

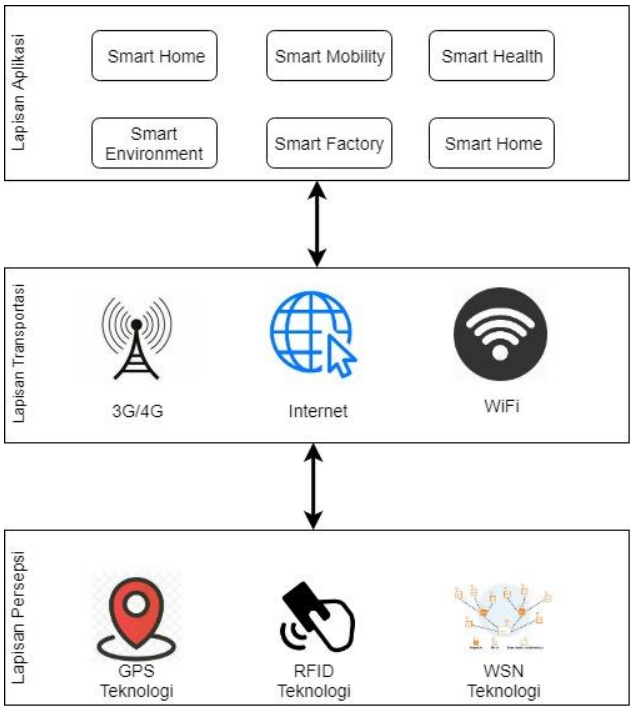
Dalam penelitian menunjukkan presentase penggunaan perangkat pintar yang diretas pada Tahun 2017 seperti yang terlihat pada gambar berikut[7]


Gambar 3. Presentase Perangkat Pintar yang diretas Tahun 2017

Peretasan perangkat pintar bisa dikarenakan beberapa hal seperti:

1) Terlalu banyak data
2) Profil public yang tidak diinginkan
3) Menguping
4) Kepercayaan konsumen

System IoT dapat direpresentasikan dan dijelaskan dalam 3 lapisan utama yakni lapisan persepsi, lapisan transportasi dan lapisan aplikasi. Masing – masing lapisan tersebut memiliki teknologi-teknologi yang berbeda-beda dan kelemahan dari segi keamanan.




Gambar 4. Model system IoT [ 9 ]

1) Lapisan Persepsi

Lapisan ini berkaitan dengan fisik sensor IoT yang mendukung pengumpulan dan pemrosesan data dari berbagai teknologi yang dimanfaatkan, seperti *radio-frequency identification*(RFID), *Wireless Sensor Network*(WSN), *RFID Sensor Network*(RSN) dan GPS. Lapisan ini termasuk sensor dan akuator dalam menunjukkan berbagai pengukuran seperti suhu, akselerasi, kelembaban, dan lain-lain.

2) Lapisan Transportasi

Lapisan transportasi menyediakan berbagai macam akses untuk lapisan persepsi. Tujuan dari lapisan ini adalah untuk mengirimkan informasi yang telah dikumpulkan dari lapisan persepsi untuk dikirimkan ke system informasi tertentu melalui jaringan komunikasi yang digunakan seperti 3G, WiFi atau jaringan internet.

3) Lapisan Aplikasi

Lapisan aplikasi menyediakan layanan yang diminta oleh pelanggan, misalnya pada lapisan ini dapat memberikan informasi mengenai pengukuran suhu dan kelembaban udara sesuai dengan data apa yang diminta oleh pengguna. Lapisan ini sangat penting dalam IoT karena mampu menyediakan informasi yang berkualitas sesuai dengan kebutuhan pengguna untuk mendukung semua jenis layanan bisnis dan untuk mewujudkan perhitungan cerdas dan alokasi sumber daya yang dapat diimplementasikan di seluruh *middleware* dan platform komutasi awan.

Tabel 1. Ancaman dalam system IoT[9]

| **Lapisan** | **Ancaman** |
|---|---|
| Lapisan Aplikasi | Kebocoran Data |
| | Serangan DoS |
| | Injeksi kode berbahaya |
| Lapisan Transportasi | Serangan Routing |
| | Serangan Routing |
| | Serangan Transit Data |
| Lapisan Persepsi | Serangan Fisik |
| | Peniruan |
| | Serangan DoS |
| | Serangan Routing |
| | Serangan Transit Data |

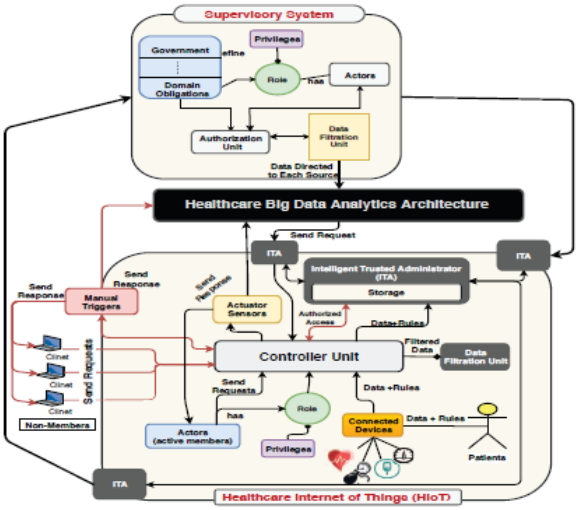
Keamanan dan privasi saling berkaitan satu sama lain, perlindungan privasi nyaris tidak mungkin dilakukan sama sekali tanpa adanya keamanan.

*C. Manajemen Energi*

Masa pakai baterai pada perangkat IoT menimbulkan banyak kekhawatiran bagi produsen perangkat dan komunitas penelitian, hal ini dikarenakan sebagian perangkat ditempatkan di lingkungan luar dan terpencil di luar jangkauan manusia sehingga terkadanhg pengisian baterai dan pengisian ulang tidak mungkin dilakukan. Perancangan protocol yang hemat energy terus banyak dilakukan termasuk pengembangan mekanisme perangkat yang dapat menghasilkan, menggunakan, mendaur ulang dan menyimpan energy dengan sendirinya. Hal ini juga termasuk pemilihan protocol yang digunakan sebagai salah satu langkah efisiensi energy, karena biasanya penggunaan protocol menghasilkan konsumsi daya yang tinggi seperti pada IEE 802.11, Bluetooth dan DECT [3]

## IV. SURVEY

Penelitian [10] mengusulkan system keamanan yang komprehensif dan arsitektur privasi yang diimplementasikan pada HIoT. Context-Sensitive Role-Based Access Control(CRBAC) yang menggabungkan peran, atribut dan konteks untuk merumuskan kondisi konteks pengontrolan akses dan jaringan. Dalam penelitian tersebut juga diusulkan sensor dan perangkat medis untuk membuat HIoT tahan terhadap serangan dari sumber – sumber yang dicurigai.




Gambar 5. Arsitektur Privasi dan Keamanan untuk HIoT

Dalam penelitian [11] mengusulkan IoT yang *lightweight* dana aman melalui mekanisme pemantauan jarak jauh menggunakan DNS dan mengevaluasi system prototipe melalui jaringan virtual. Berdasarkan evaluasi yang telah dijalankan menunjukkan hanya pengguna yang diijinkan saja yang dapat mendapatkan data IoT, dengan hasil tersebut diharapkan dapat memcahkan masalah yang ada dengan solusi konvensional memanfaatkan protocol DNS. Penggunaan protocol DNS untuk pemantauan jarak jauh pada IoT memilki beberapa manfaat penting diantaranya kesesuaian, skalabilitas, komunikasi yang aman dan privasi.

Penelitian [12] menganalisa pola konsumsi energy MCU berbasis FRAM sesuai dengan konfigurasi tugas memori. Konsumsi energi keseluruhan dari perangkat IoT dapat dikurangi dengan mengurangi energy yang dikonsumsi dalam mengakses memori. Semakin lama waktu pelaksanaan tugas, maka semakin sedikit energy yang dikonsumsi dalam pemetaan SRAM. Jika ada banyak data untuk bermigrasi dan durasi mode *sleep* pendek, *sleep mode* yang pendek dapat mengurangi konsumsi energy. Jika jumlah dari data yang akan dimigrasi kecil dan durasi mode *sleep* panjang, maka dapat mengurangi konsumsi energi juga. Dengan mempertimbangkan *overhead* data migrasi, aka nada penghematan energy mencapai 50% jika konfigurasi memori optimal yang dipilih.

Dalam penelitian [13] diinplementasikan versi cahaya dari kurva elips yang sesuai dengan algoritma untik IoT, algoritma yang sesuai tersebut diuji pada 2 mikrokontroller yang berbeda yang berbasis AVR dan MSP430. Kecepatan dari ekseskusi algoritma disamakan dengan mengubah nilai optimasi, pemilihan model kurva dan model aritmatikanya. Algoritma yang diusulkan adalah untuk menyelesaikan permasalahan sistem IoT terkait batasan penggunaan sumber daya. Ada 2 jenis algoritma berbeda yang diterapkan dalam penelitian ini:

- Algoritma yang membutuhkan lebih banyak kode program dan lebih banyak sumber daya untuk melakukan ekseskusi, dan
- Algoritma yang lebih lambat dan membutuhkan lebih dikit sumber daya

Kedua algoritma tersebut bersifat *real-time* dan dapat bertahan. Algoritma ECC dikembangkan ulang dan dioptimalkan pada node MICAz dan Tmote Sky.

Penelitian [14] diimplementasikan skema kriptografi yang tahan kuantum pada perangkat IoT. Hal ini dikarenakan pada penelitian – penelitian terdahulu menunjukkan adanya pengaruh daya computer kuantum terutama pada algoritma kriptografi yang saat ini banyak digunakan. Untuk itu dibutuhkan algoritma yang dapat tahan terhadap kuantum dalam perangkat IoT. Tantangan terbesar yang dihadapi tidak hanya perlindungan dari keamanan perangkat IoT, tetapi juga pada penerapan kekuatan kuantum dalam teknologi IoT.

Dalam penelitian [15] membentuk suatu kerangka yang dapat mengurangi biaya enkripsi data dengan menghindari perhitungan yang berketergantungan. Pada penelitian ini diusulkan teknik baru untuk menyerang enkripsi multi-key Cui yang memungkinkan pengguna jahat dapat menemukan kunci pengguna yang sah dari kunci pengguna yang tidak sah

Dalam survey yang dilakukan menunjukkan bahwa sudah banyak pendekatan yang telah dihasilkan dan signifikan dari penelitian – penelitian terdahulu. Ada sejumlah algoritma yang memiliki peran penting dalam keamanan di dalam bidang IoT seperti RSA kriptografi, computer kuantum, MOTE-ECC dan pengaruh Fog dalam IoT[2].

Pada penelitiannn [16] menjelaskan peran IoT yang terdiri dari sensor – sensor dalam Kota Cerdas, yang secara terus menerus mengumpulkan data yang dibutuhkan untuk disimpan, preprosesing, diolah dan dianalisa sebelum diterapkan diberbagai tempat yang menyediakan layanan intelijen untuk mendukung konsep Kota Cerdas secara real-time. Bagaimana mengintegrasikan teknologi – teknologi baru dan konsep-konsep seperti Internet Of Things, big data dan interkoneksi energy sehingga dapat membantu perkembangan Kota Cerdas.

Setelah menganalisa kesulitan – kesulitan di IoT, big data dan energy internet dan membandingkan persamaan dan perbedaan nya ddengan blockchain, maka analisis tersebut menunjukkan bahwa secara teknis karakteristik blockchain cocok untuk energy internet, memechkan masalah jaringan dan big data seperti tingginya biaya untuk pemelihraan database terpusat, kebocoran privasi pengguna dan sebagainya.

Tabel 2. perbedaan antara blockchain dengan energy internet[16]

| Fitur | Energi Internet | Blockchain |
|---|---|---|
| Terbuka | Struktur jaringan terbuka untuk semuanya dan menyediakan platform untuk bertukar informasi | Menyediakan berbagai macam antar muka jaringan, terutama untuk bergabung dan sintesis dari database yang terdistribusi |
| Peer | Setiap bagian dari jaringan dapat mengatur konsumsi energinya sendiri dan bertransaksi secara mandiri dan berpartisipasi dalam pengambilan keputusan | Dengan karakteristik pemeliharaan yang desentralisasi dan kolektif, pengoperasian system tidak terdapat di pusat control, tetapi itu merupakan pengambilan keputusan yang terdesentralisasi |

| | | |
|---|---|---|
| | | dari setiap node. |
| Sharing | Setiap modul system dapat mencapai interkoneksi energy dan informasi secara penuh dengan keamanan dan ekonomi yang tinggi | Sebagai jaringan yang terdistribusi dengan interkoneksi node secara realtime dan penyimpanan data yang berlebihan dan berbagi |
| Interkoneksi | Berbagi informasi tentang system operasi dan transaksi antar node bisa bisa ditingkatkan dengan mengoptimalkan alokasi sumber daya | Inti dari blockchain adalah database terdistribusi. Semua node dalam jaringan P2P saling berbagi informasi semua blok di saat yang bersamaan untuk memastikan keamanan dan transparansi dari sisem operasi. |

Blockchain sulit untuk diserang dan 51% dari serangan adalah berbiaya tinggi, apa yang dapat dilakukan penyerang hanya bisa mengubah kesepakatan dirinya sendiri dan transaksi terakhir saja.

Beberapa permasalahan IoT yang dapat diselesaikan oleh blockchain:

1) Sertifikasi identitas pada node IoT

   Verifikasi blockchain dan mekanisme consensus membantu mengidentifikasi node IoT mana saja yang sah dan menghindari akses yang berbahaya terhadap node perangkat

2) Masalah privasi dan keamanan data IoT

   System data di blockchain adalah terdistribusi(tidak terpusat), dengan setiap node sama dan semua data dienkripsi.

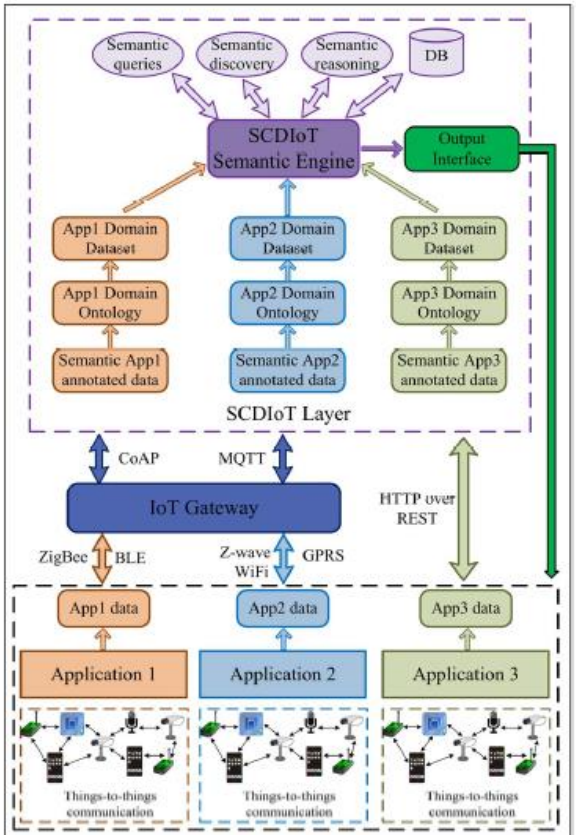
3) Database terpusat itu mahal dan kemampuan komputasi dan penyimpanan terbatas

4) Pemeliharaan dan peningkatan peralatan IoT

Contoh penggunaan blockchain dalam kehidupan sehari –hari, informasi lalu lintas yang sekarang membutuhkan transit lewat pusat data, dengan demikian mengurangi ketepatan waktu dan keakuratan informasi. System blockchain dibangun dari titik ke titik, ujung ke ujung , masing – masing mobil memeliki identitas unik masing – masing. Kendaraan akan melaporkan posisinya secara realtime, melalui peralatan jaringan pada kendaraan untuk menangkap data kendaraan di sekitarnya.bisa merencanakan rute terbaik saat ini.

Dalam penelitian [17] menyajikan sirkuit SRAM berdaya sangat rendah yang cocok digunakan untuk mikrokontroller IoT yang berbiaya ketat dengan teknik reduksi pada kebocoran daya menggunakan pengaturan ganda tegangan footer dan header yang diatur ganda dengan tujuan untuk memenuhi kebutuhan penyimpanan data SRAM di aplikasi IoT. Membandingkan single regulated footer voltage(SRFV), singl regulated header voltage(SRHV) dan double regulated footer and footer voltage(DRFHV). Teknik DRFHV menunjukkan sebagai kandidat teknik yang paling menjanjikan untuk konsumsi daya yang lebih rendah dalam desain SRAM setelah dianalisis dalam berbagai tegangan suplai, suhu dan waktu tidur.

Penelitian [18] mengusulkan komunikasi tingkat global , Social Cross-domain IoT(SCDIoT) yang memungkinkan komunikasi antara aplikasi-aplikasi memnafaatkan hubungan sosial dan lingkaran dimanaaplikasi IoT dapat berkolaborasi antara satu sama lain. kerangka kerja yang merepresentasikan interoperabilitas, dan hubungan social sebagai pengembangan dari Social IoT (SIoT) yang memungkinkan hubungan sosial dengan cicle di IoT.




Gambar 6. Framework SCDIoT yang diusulkan[18]

Berbeda dengan pengembangan perangkat IoT secara tradisional dimana perangkat IoT tidak saling berbicara, aplikasi ini mendukung komunikasi *things-to-things* dimana perangkat juga saling berbicara satu sama lain dengan saling bersosialisasi dengan mengaktifkan oleh SIoT. Kerangka kerja ini bisa digunakan dalam berbagai scenario, seperti menghitung suhu ruangan dimana berbagai sensor suhu dipasang dalam sebuah ruangan. Sensor dapat berkoordinasi dan berkolaborasi satu sama lain untuk memperbaiki akurasi penukuran mereka. Misalnya jika ada 4 sensor suhu ditempatkan di sebuah ruangan dan 3 dari sensor tersebut mengukur jika suhu ruangan tersebut adalah 20 derajat celcius sedangkan ada 1 sensor yang mengukur suhu ruangan tersbut adalah 4 derajat Celsius, hal ini menunjukkan adanya masalah dengan sensor keempat. Sensor keempat akan mengidentifikasi masalah ini dan juga tiak akan meneruskan informasi tersebut ke gateway atau akan mengambil pengukuran lagi. Komunikasi yang didukung oleh SIoT menghadirkan komputasi satu tingkat lebih rendah, seperi dari cloud ke edge menjadi things-to-things.

Setiap aplikasi mengumpulkan data lalu diteruskan ke lapisan SCDIoT untuk mengaktifkan aplikasi sosialke aplikasi komunikasi. Penerusan data dapat dicapai melalui berbagai protocol heterogen, seperti Constrained Application Protocol(CoAP) atau Message Queuing Telemetry Transport(MQTT).

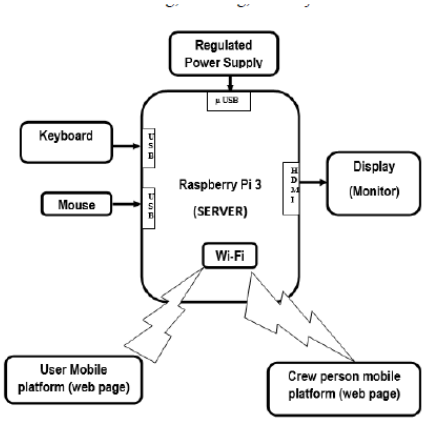
Tantangan terbesar dalam system SCDIoT adalah latensi , karena komunikasi aplikasi ke aplikasi sosial sangat dimungkinkan melalui kerangka kerja SCDIoT, lebih banyak latensi yang dapat terjadi karena data terlebih dahulu harus dikirim ke SCDIoT yang melakukakan pemrosesan dan kemudian mengirim kembali informasi yang diperlukan oleh aplikasi. Oleh karena itu ini menjadi tantangan yang cukup serius ketika berhubungan dengan system kesehatan misalnya.

Penelitian [18] model protipe berbasis IoT yang dikembangkan untuk memberikan layanan kepada setiap penumpang kereta api yang sedang bergerak. setiap kompertmen/gerbong masing - masing akan diinstal perangkat IoT menggunakan raspberry pi, satu diantaranya berperan sebagai server. Raspberry Pi bertanggungjawab untuk menyediakan komunikasi nirkabel antara penumpang dan server. algoritma CSM membutuhkan waktu minimal penundaan untuk memenuhi kebutuhan penumpang jika dibaningkan algoritma sebelumnya menggunakan handphone,bluetooth beacon server yang berisi daftar sumber daya segmen mana saja dan mendistribusikan beban kerja dibagi sama rata kepada semua awak. semua kebutuhan penumpang deisediakan sumber daya yang sesuai tanpa keterlambatan.

Coposite schedule for multitask(CSM) algoritma dijalankkan berulang kali setiap 100 detik. Langkah – langkah eksekusi algoritma CSM adalah sebagai berikut:

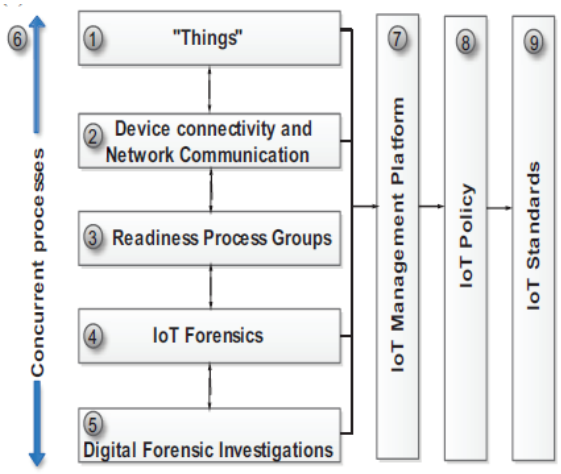
- Di setiap kompartemen ditempatkan raspberry pi dan satu diantaranya akan menjadi master
- Setiap model pi pada setiap kompartemen akan menerima permintaan secara acak dari platform seluler penumpang
- Setelah permintaan dikumpulkan di raspberry pi, maka mulai membuat database baru(daftar sumber daya)yang ditetapkan sebagai daftar prioritas. Jika ada 2 permintaan punya prioritas yang sama, maka prioritas diberikan berdasarkan jam kedatangan
- Daftar segmen server disiapkan sebagai daftar sumber daya oleh algoritma CSM dan menugaskan masing – masing segmen untuk setiap awak
- Jika permintaan baru dibuat saat algoritma sedang berjalan, maka master akan memeriksa prioritas permintaan yang baru tiba dan jika kemudian memiliki prioritas yang lebih tinggi, segera memberikan tugas tersebut
- Setelah tugas awak selesai, maka dia perlu tetap ada di sana sampai segmen baru tiba sebaliknya.

Konsep otomasi di kereta akan meningkatkan kepuasan pelanggan dan juga meningkatkan profit kepada pemerintah di masa mendatang.



Gambar 7. Blok Diagram yang diusulkan[19]

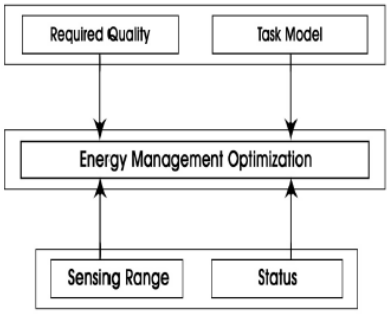
Integrated Digital Forensic Investigation Framework(IDFIF-IoT) adalah salah satu kontribusi IoT berbasis ekosistem. Ekosistem yang dimaksud adalah satu set hubungan yang kompleks dianatara berbagai hal, seperti satu set hubungan antara sensor, actuator dan juga benda – benda pintar. Konsep ini membuat aplikasi dapat semakin cerdas, dapat deprogram dan lebih mampu berinteraksi satu sama lain.IDFIF-IoT menggunakan *high level* seperti pada gambar dibawah.[19]




Gambar 8. *High level* IDFIF-IoT[19]

Setelah dievaluasi, IDFIF-IoT dapat digunakan dengan mudahsebagai dasar dari konsep investigasi tingkat tinggi beradasrkan ekosistem. Kerangka kerja dapat dengan mudah mengatasi masalah investigasi digital sejak standar ISO/ICE 27043 diterapkan juga dalam kerangka kerja.

Penelitian [21] mengusulkan jika system dibagi kedalam 3 modul utama yaitu sensor ranges, task module dan energy management seperti tergambar pada gambar 7 dibawah. Task module digunakan untuk menghitung berbagai jenis tugas untuk node sensor saling berkomunikasi dengan simpul sensor lainnya, menghitung jarak komunikasi dan menghitung cluster didasarkan pada konsumsi energy dari estimasi energy setiap node. Jaringan sensor dengan factor pemilihan tertinggi dengan energy terndah, dianggap sebagai solusi manajemen energy paling optimal.




Gambar 8. Sistem yang diusulkan [21]

System yang diusulkan diatas adalah efisiensi energy dan dapat beradaptasi sendiri berdasarkan perkembangannya dalam Energiy efficient Internet of Things(EEIoT). Strategi pengoptimalan energi terdiri dari 3 fase. Pada tahap pertama sensor ada di optimasi *hard level*, tahap selanjutnya manajemen dan optimisasi dilakukan untuk mengontrol dan mengelola energi, tahap terakhir didasarkan pada tugas dan kualitas bisa juga meningkatkan power yang ada tanpa memanfaatkan alternative energi lainnya.

EEIoT merupakan metode pengumpulan energi terbaik yang dioptimalkan dengan teknik *self-adaptive* dan pengurangan energi jika ndibandingkan dengan metode tradisional. EEIoT akan banyak membantu menjaga kekuatan yang tersedia untuk jangka waktu yang lama untuk permasalahan seperti sensor yang ada di tempat terpencil jauh dari jangkauan manusia. System yang diusulkan hanya berbasis komunikasi dan kurangnya energi yang tersedia.

## KESIMPULAN

Penelitian – penelitian yang sudah ada menunjukkan jika permasalahan mengenai privasi, keamanan dan manajemen energi masih menjadi fokus utama dalam perkembangan IoT di masa depan. Hal ini seiring dengan semakin banyaknya perangkat – perangkat IoT yang sudah terpasang, menjadikan pertukaran data dan penggunaan energi semakin besar.

IoT juga sebagai salah satu teknologi yang sering digunakan dalam pengembangan konsep kota cerdas di beberapa negara, menimbulkan masih banyaknya peluang – peluang yang dapat dipelajari lebih lanjut dalam perngembangan IoT di masa depan baik dari segi aplikasi, teknologi, strategi maupun bisnis.

Di masa depan IoT dan kota cerdas menjadi teknologi yang tidak terpisahkan satu sama lain, karena manusia akan semakin bergantung pada IoT dalam kehidupan sehari-hari.

## REFERENSI


[1] Perera, C., Member, S., Zaslavsky, A., Christen, P., and Georgakopoulos, D. (2014): Context Aware Computing for The Internet of Things : A Survey, *IEEE Communications Surveys & Tutorials*, **16**(1), 414–454. https://doi.org/10.1109/SURV.2013.042313.00197

[2] Chernyshev, M., Baig, Z., Bello, O., and Zeadally, S. (2018): Internet of Things ( IoT ): Research ,, *IEEE Internet of Things Journal*, **5**(3), 1637–1647. https://doi.org/10.1109/JIOT.2017.2786639

[3] Ahlgren, B., Swedish, S., Hidell, M., and Royal, K. T. H. (2016): Internet of Things for Smart Cities : Interoperability and Open Data, *IEEE Internet Computing*, **20**, 52–56. https://doi.org/10.1109/MIC.2016.124

[4] Eckhoff, D., and Wagner, I. (2018): Privacy in the Smart City — Applications , Technologies , Challenges , and Solutions, *IEEE Communications Surveys & Tutorials*, **20**(1), 489–516. https://doi.org/10.1109/COMST.2017.2748998

[5] Tay, K. K. C., Cornelius, G., and Arman, A. A. (2018): The SMART Initiative and the Garuda Smart City Framework for the Development of Smart Cities, *2018 International Conference on ICT for Smart Society (ICISS)*, (April), 1–10.

[6] Solangi, Z. A., Solangi, Y. A., Chandio, S., Aziz, S. A., and Syarqawy, M. (2018): The future of data privacy and security concerns in Internet of Things, *2018 IEEE International Conference on Innovative Research and Development (ICIRD)*, (May), 1–4. https://doi.org/10.1109/ICIRD.2018.8376320

[7] Hassan, A. M., and Awad, A. I. (2018): Urban Transition in the Era of the Internet of Things : Social Implications and Privacy Challenges, *IEEE Access*, **6**, 36428–36440. https://doi.org/10.1109/ACCESS.2018.2838339

[8] Frustaci, M., Pace, P., and Aloi, G. (2018): Evaluating Critical Security Issues of the IoT World : Present and Future Challenges, *IEEE Internet of Things Journal*, **5**(4), 2483–2495. https://doi.org/10.1109/JIOT.2017.2767291

[9] Alagar, V., Alsaig, A., and Ormandjieva, O. (2018): Context-based Security and Privacy for Healthcare IoT. https://doi.org/10.1109/SmartIoT.2018.00-14

[10] Jin, Y., and Tomoishi, M. (n.d.): A Lightweight and Secure IoT Remote Monitoring Mechanism Using DNS with Privacy Preservation, *2019 16th IEEE Annual Consumer Communications & Networking Conference (CCNC)*, 1–2.

[11] Kim, M., Lee, J., Kim, Y., and Song, Y. H. (2018): An Analysis of Energy Consumption under Various Memory Mappings for FRAM-based IoT Devices, *2018 IEEE 4th World Forum on Internet of Things (WF-IoT)*, 574–579. https://doi.org/10.1109/WF-IoT.2018.8355212

[12] Liu, Z., Huang, X., Hu, Z., Khan, M. K., Seo, H., and Zhou, L. (2017): On Emerging Family of Elliptic Curves to Secure Internet of Things : ECC Comes of Age, *IEEE Transactions on Dependable and Secure Computing*, **14**(3), 237–248. https://doi.org/10.1109/TDSC.2016.2577022

[13] Cheng, C., Lu, R., Petzoldt, A., and Takagi, T. (2017): Securing the Internet of Things in a Quantum World, *IEEE Communications Magazine*, **55**(February), 116–120. https://doi.org/10.1109/MCOM.2017.1600522CM

[14] Zhou, R., Zhang, X., Du, X., Wang, X., Yang, G., and Guizani, M. (2018): File-Centric Multi-Key Aggregate Keyword Searchable Encryption for Industrial Internet of Things, *IEEE Transactions on Industrial Informatics*, **14**(8), 3648–3658. https://doi.org/10.1109/TII.2018.2794442

[15] Shuling, L. (2018): Application of Blockchain Technology in Smart City Infrastructure, *2018 IEEE International Conference on Smart Internet of Things (SmartIoT)*, 276–2766. https://doi.org/10.1109/SmartIoT.2018.00056

[16] Vo, H. M. (n.d.): A Double Regulated Footer And Header Voltage Technique For Ultra-Low Power IoT SRAM, *2018 IEEE 4th World Forum on Internet of Things (WF-IoT)*, 107–111. https://doi.org/10.1109/WF-IoT.2018.8355203

[17] Saleem, Y., Crespi, N., and Pace, P. (2018): SCDIoT : Social Cross-Domain IoT enabling Application-to-Application Communications, *2018 IEEE International Conference on Cloud Engineering (IC2E)*, 346–350. https://doi.org/10.1109/IC2E.2018.00068

[18] Hussain, S. A., and Ramaiah, C. S. (2019): IOT Multitasking : Design of Smart phone application for systematic execution and scheduling in real time environment, *2019 4th MEC International Conference on Big Data and Smart City (ICBDSC)*, 1–6.

[19] Kebande, V. R. (2020): Towards an Integrated Digital Forensic Investigation Framework for an IoT-Based Ecosystem, *2018 IEEE International Conference on Smart Internet of Things (SmartIoT)*, 93–98. https://doi.org/10.1109/SmartIoT.2018.00-19

[20] Sadeeq, M. A. M. (2018): Internet of Things Security : A Survey, *2018 International Conference on Advanced Science and Engineering (ICOASE)*, 162–166.

[21] Suresh, K. (2016): EEIoT : Energy Efficient mechanism to leverage the Internet of Things ( IoT ), *2016 International Conference on Emerging Technological Trends (ICETT)*, 1–4. https://doi.org/10.1109/ICETT.2016.7873689