ITEJ Juli-2020, Volume 5 Nomor 1 Page 25 - 36

ITEJ
Information Technology Engineering Journals
eISSN : 2548-2157

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

Survey of Future Internet of Thing

Hani Purwati Hanifah
School of Electrical Engineering and Informatics
Institute of Technology, Bandung (ITB)
Bandung, Indonesia
hanipurwatihanifah@gmail.com

***Abstract*— The Internet of Things is a technology that will become an integral part of human life. At present, its use has begun to be widely applied in various scientific fields such as agriculture, health, industry, etc. so that it has a very good impact. In addition, the development of this device has also reached a point where collaboration with various scientific fields has occurred. However, in addition to the benefits offered by the Internet of Things, there are challenges such as the use of energy in data transfer, memory limitations and so on as well as threats that can arise such as loss of privacy, leakage of data and information, or use to commit crimes in the physical world.**

Keywords—Future, Internet of Things, IoT

I. INTRODUCTION

Internet of Things atau lebih dikenal dengan sebutan IoT menjadi sebuah pilihan solusi yang menjanjikan dalam mengubah operasi dan peran di berbagai bidang. Diantaranya ketika digunakan dalam bidang kesehatan, IoT digunakan untuk memantau detak jantung, kadar kolesterol, gula darah dan indikator kesehatan lainnya sehingga dapat diupayakan tindakan pencegahan terjadinya resiko kesehatan. Dalam bidang transportasi, IoT dapat menciptakan sistem cerdas yang dapat berkomunikasi dengan infrastruktur kota seperti lampu lalu lintas sehingga dapat melacak kendaraan dengan memonitor pergerakan dan lokasi kendaraan tersebut serta dapat memprediksi jalur yang dapat diambil berdasarkan lalu lintas jalan. Peran IoT pada Kota Cerdas adalah ketika menghubungkan berbagai infrastruktur kota seperti lampu lalu lintas, penerangan jalan, sensor yang mendeteksi getaran gedung dan jembatan, dan sensor lainnya sehingga dapat dimanfaatkan untuk optimalisasi penggunaan energi, diagnosis masalah struktural dan memprediksi waktu kerusakan yang setiap infrastruktur sehingga dapat mencegah bencana yang mungkin ditimbulkan dari kerusakan infrastruktur kota. Pada bidang industri, IoT dapat digunakan pada sistem produksi atau manufaktur, inventori, distribusi dan pemasaran. Bidang lainnya yang terkena dampak IoT ini adalah pertanian, peternakan, pendidikan, pemerintahan, perdagangan dan sebagainya.

IoT merupakan teknologi yang terkait dengan teknologi jaringan sensor nirkabel yang di dalamnya terdapat sensor, aktuator, perangkat GPS dan seluler [1]. Perangkat seluler atau bisa juga menggunakan Wifi, digunakan sebagai perangkat untuk komunikasi atau pengiriman data. Jadi IoT dapat digambarkan sebagai infrastruktur global yang memungkinkan layanan lanjutan yang dapat dioperasikan dan dikembangkan dengan menghubungkan berbagai hal baik fisik maupun virtual berdasarkan teknologi informasi dan komunikasi [2].

Ada berbagai penelitian yang telah dilakukan terkait IoT karena IoT mulai digunakan dalam kehidupan sehari-hari sehingga memunculkan ide-ide penggunaan teknologi IoT pada berbagai

perangkat yang terkait kebutuhan atau aktifitas masyarakat saat ini. Makalah ini mengumpulkan berbagai penelitian yang pernah dilakukan terkait IoT yang mungkin digunakan di masa yang akan datang. Tidak bisa dipungkiri lagi, di masa yang akan datang IoT tidak dapat dipisahkan lagi dari kehidupan manusia.

II. FUTURE IOT

Michele Zorzi, Alexander Gluhak, Sebastian Lange, dan Alessandro Bassi [3] membahas status dan deskripsi Internet of Things saat ini dikaitkan dengan situasi di banyak "Intranet" of Things yang harus berkembang menjadi sistem yang terintegrasi dan heterogen. Selain itu, artikel ini juga merangkum tantangan teknis utama yang berhubungan dengan nirkabel dan mobilitas serta menguraikan beberapa gagasan awal tentang solusi untuk mengatasi tantangan tersebut sehingga dapat memfasilitasi pengembangan dan penerimaan IoT dimasa yang akan datang. Adapun studi kasus yang dijelaskan adalah tentang arsitektur protokol IoT. Namun masih banyak masalah teknis utama lainnya yang belum terpecahkan, termasuk heterogenitas, skalabilitas, keamanan, konektivitas, energi, manajemen, penamaan dan identifikasi. Kompleksitas masalah teknis ini terutama pada sifat sumber daya yang terbatas dari banyak komponen IoT dan penggunaan komunikasi nirkabel, sehingga membutuhkan arsitektur terpadu yang dapat mengatasinya secara koheren.

Huansheng Ning dan Ziou Wang [4] pada makalahnya membahas arsitektur IoT masa depan dari dua aspek yaitu Unit IoT dan Ubiquitous IoT. Pada Unit IoT, arsitekturnya dibangun dari model Man Like Neural Network (MLN) dan modifikasinya. Sedangkan Ubiquitous IoT mengacu pada IoT global atau integrasi dari beberapa IoT Unit dengan karakter "ubiquitous", sedangkan arsitekturnya menggunakan model kerangka kerja organisasi sosial atau social organization framework (SOF). Model ini disebutkan dapat membantu menjelaskan hubungan antara IoT dengan dunia nyata serta bermanfaat dalam penerapan IoT saat ini. Makalah ini juga memperkenalkan definisi Unit IoT dan Ubiquitous IoT dengan menggambarkan arsitektur yang dibangunnya dengan model MLN dan SOF, sehingga ditemukan masalah yang paling signifikan yaitu interkoneksi & intra-koneksi, dan kompatibilitas. Masalah utama lainnya yang ditemukan adalah standar arsitektur IoT, yaitu bagaimana beberapa standar global, industri, atau regional dapat dibangun berdasarkan persyaratan interkoneksi & intra-koneksi dan kompatibilitas.

Muhammad S. Khan, Mohammad S. Islam, dan Hai Deng [5] pada makalahnya memperkenalkan rangkaian atau tag penginderaan Radio Frequency Identification (RFID) UHF semi pasif dan dapat dikonfigurasi ulang yang beroperasi sebagai platform penginderaan umum atau the generic sensing platform (GSP) dan simpul penginderaan dari IoT masa depan. Platform ini menawarkan beberapa sensing channels yang murah dan bersifat plug-and-play untuk sensor fisik tambahan pada pengambilan data secara real-time. Perangkat ini dapat dikonfigurasi secara dinamis sehingga dapat beroperasi dengan baik dalam mode online sebagai platform transmisi data kontinu maupun dalam mode offline sebagai platform logging data. Saat menggunakan mode offline, untuk mengelola dan mengakomodasi data bervolume tinggi yang diperoleh dari perangkat sensor maka segera dirancang dan diimplementasikan skema manajemen memori. Platform ini juga menggunakan strategi komunikasi data yang inovatif dan kompatibel dengan protokol komunikasi pada electronic product code (EPC) Gen-2 saat ini untuk memfasilitasi komunikasi data sensor dan pertukaran informasi lainnya antara the sensing node dan the routing tier of IoT. Hasil dari platform yang dirancang pada makalah ini dapat digunakan dan diuji dalam pengaturan percobaan IoT untuk evaluasi kinerjanya sebagai GSP karena mampu mempresentasikan desain, implementasi dan hasil pengujian dari tag penginderaan RFID semi konfigurasi ulang yang berfungsi sebagai GSP pada IoT masa depan. Platform penginderaan dinamis yang diperkenalkan di makalah ini dapat dikonfigurasi ulang serta menawarkan modularitas sensor yang fleksibel. Selain itu, tag-GSP ini memiliki keunggulan dibandingkan tag penginderaan lainnya sebagai node sensor generik dalam desain dan pengembangan IoT di masa depan.

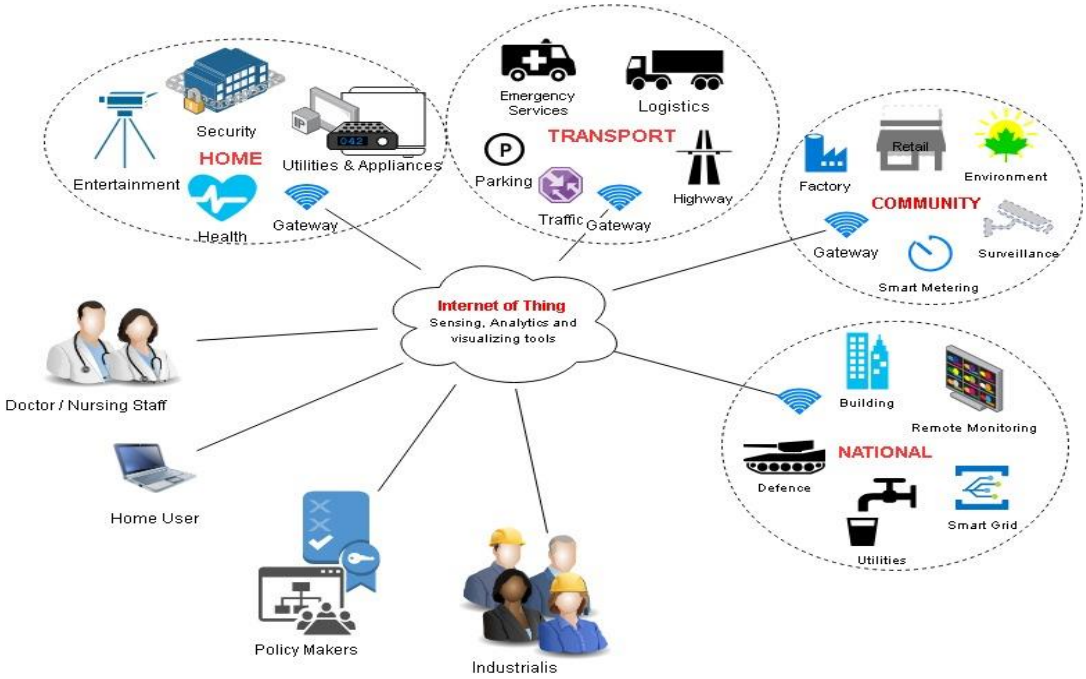
Kazi Masudul Alam, Mukesh Saini, dan Abdulmotaleb El Saddik [6] pada makalahnya memperkenalkan visi utama dari IoT, yaitu untuk melengkapi objek fisik di kehidupan nyata dengan menggunakan kemampuan komputasi dan komunikasi sehingga antar perangkat dapat berinteraksi satu sama lain untuk manfaat sosial. Internet of Vehicle (IoV) yang merupakan bagian IoT telah mengalami

kemajuan pesat dalam teknologi komunikasinya, sehingga antar kendaraan dan infrastrukturnya dapat bertukar informasi keselamatan, efisiensi, infotainment, dan kenyamanan dengan menggunakan vehicular ad hoc networks (VANETs). Makalah ini juga mengusulkan arsitektur cyber-fisik untuk Social IoV (SIoV) yang memanfaatkan tema VANET berbasis cloud dan merupakan contoh kendaraan dari Social IoT (SIoT) dimana kendaraan adalah entitas sosial utama dalam jaringan sosial kendaraan machine-to-machine. Struktur sosial komponen SIoV, hubungan mereka, dan jenis interaksi telah diidentifikasi. Komponen VANET dipetakan menjadi model referensi arsitektur IoT-A dan menawarkan integrasi SIoV yang lebih baik dari domain IoT lainnya. Struktur pesan komunikasi disajikan berdasarkan ontologi otomotif, set pesan SAE J2735 dan skema sistem informasi perjalanan canggih yang terjadi dan disesuaikan dengan dengan grafik sosial. Selain itu, makalah ini merinci Social Internet of Vehicles sebagai kasus menarik dari Social Internet of Things, menjelaskan detail implementasi dari struktur pesan, analisis ukuran payload, pendekatan implementasi infrastruktur fisik-cyber dan simulator IoV menggunakan jejak SUMO, Open Street Map, dan OBD2. Terdapat skenario aplikasi prototipe yang dimasukkan ke dalam kelompok pengguna yang berbeda seperti pengemudi, penumpang, pengguuna web sosial dan otoritas transportasi sehingga dapat dibayangkan bahwa SIoV akan menjadi bagian terintegrasi dari sistem transportasi cerdas di Kota Pintar masa depan. Untuk mewujudkan SIoV ini, ada beberapa masalah penting yang perlu dipertimbangkan seperti skalabilitas, redundansi data, dan sinkronisasi. Karakteristik beban kerja dari SIoV juga harus dirinci agar dampak muatan pada infrastruktur VANETs dapat dipahami.

Dejan Vukobratovic, Dusan Jakovetic, Vitaly Skachek, Dragana Bajovic, Dino Sejdinovic, Güne Karabulut Kurt, Camilla Hollanti, dan Ingo Fischer [7] menjelaskan dalam makalahnya bahwa IoT pada tahun-tahun yang akan datang akan menghubungkan miliaran perangkat pintar yang dapat menghasilkan dan mengunggah data sehingga membanjiri cloud. Ketika pengetahuan atau Knowledge yang terkubur di dalam data berhasil diekstraksi, maka dapat meningkatkan kualitas hidup dan mendorong pertumbuhan ekonomi secara signifikan. Namun terdapat hambatan kritis dalam mewujudkan IoT yang efisien. Hambatan ini adalah tekanan yang diberikan pada infrastruktur komunikasi saat ini membutuhkan kemampuan transfer volume data yang sangat besar. Untuk mengatasi hambatan ini, makalah ini mengusulkan arsitektur baru yang dinamai Condense, yaitu arsitektur yang mengintegrasikan infrastruktur komunikasi IoT ke dalam analisis data yang dicapai melalui konsep generik fungsi jaringan komputasi. Pada arsitektur ini, selain mentransfer data dari sumber IoT ke Cloud, infrastruktur komunikasi juga berpartisipasi aktif dalam analisis data dengan merancang proses en-route secara cermat. Makalah ini mendefinisikan juga arsitektur, lapisan dasar dan interaksi diantara modul-modul penyusun Condense, menjelaskan bagaimana Condense dapat diintegrasikan ke dalam arsitektur Third Generation Partnership Project (3GPP) machine type communications (MTCs) serta kemungkinann menjadikannya teknologi praktis dalam waktu singkat dengan mengandalkan fungsi jaringan virtualisasi dan software-defined networking.

Bill Montgomery [8] dalam artikelnya menyebutkan bahwa pada pada hari ini dan tahun 2029 atau sekitar 35 tahun setelah internet menjadi arus utama, orang-orang dan berbagai hal akan saling terkoneksi satu sama lain dengan cara yang tidak diduga sebelumnya. Internet of Thing atau yang menurut Cisco adalah Internet of Everything, sekarang menjadi kenyataan yang meningkatkan kehidupan orang-orang dengan berbagai cara. Contohnya seperti kendaraan saat ini menjadi komputer beroda yang dapat mendiagnosis diri dan berkomunikasi dengan pusat layanan sehingga dapat menjadwalkan jadwal servis, bahkan sampai dapat mengatur transportasi alternatif disaat kendaraan yang digunakan mogok. Semua kendaraan transportasi seperti mobil, bus, truk dan kereta api saling berkomunikasi dan memberikan peringatan jika terjadi masalah lalu lintas seperti kecelakaan kendaraan terdekat atau cuaca buruk di jalan. Selain itu, pada 2029 kendaraan akan saling berkomunikasi dengan infrastruktur kota mulai dari lampu lalu lintas hingga jalan raya. Dampak postiti IoT juga telah menyentuh komoditas yang paling bernilai yaitu sumber daya alam. Sebagian besar pasokan air dunia saat ini telah sepenuhnya saling terhubung, sehingga memungkinkan pemantauan kualitas air dan deteksi dini kerusakan saluran distribusi air. IoT juga berdampak positif pada sektor lainnya seperti kesehatan, pertanian, distribusi, perhutanan, dll. Pada sektor pertanian dan perhutanan, sensor digunakan untuk memantau kondisi tingkat kelembapan tanah, deteksi dini kebakaran hutan dan distribusi air untuk pengairan lahan yang mengalami kekeringan. Pada artikel ini juga disebutkan bahwa ada tiga pilar penting yang harus dipastikan terlebih dahulu agar solusi yang ditawarkan IoT

dapat digunakan secara cepat dan aman. Ketiga pilar tersebut adalah security, trust dan Identity of Things.



Gambar 1. Model otentikasi untuk aplikasi IoT [10] (diadaptasi dari [11])

Pavel M. Gotovtsev dan Andrey V. Dyakov [9] dalam makalahnya memberikan ikhtisar penerapan beberapa bioteknologi di kota cerdas dengan penggunaan IoT. Contohnya seperti penggunaan biosensor pada pengontrolan lingkungan sistem pengolahan air biologis lokal dan fotobioreaktor. Bioteknologi masa depan yang dapat menemukan aplikasi yang tepat dalam konsepsi kota pintar hijau juga ditinjau secara singkat. Saat ini, bioteknologi yang mengarah pada penerapan luas memberikan harapan baru bagi dunia yang berkelanjutan, terutama di kota hijau. Dalam artikel ini juga disebutkan beberapa bioteknologi yang sudah terintegrasi menjadi bagian dari IoT kota pintar. Ada beberapa pendekatan yang sekarang dikembangkan, diantaranya biosensor, biofuel cells, biosolar cells, bioreactors untuk efisiensi energi, green bioprinting, dan banyak lainnya yang merupakan salah satu langkah pertama bioteknologi di lingkungan kota hijau. Menjadi salah satu bagian dasar konsep kota pintar saat ini, dengan memasukkan bioteknologi kedalam konsepnya diperlukan tanjauan secara terperinci khusunya yang meliputi namun tidak terbatas pada berbagai jenis aplikasi biosensor untuk pengendalian lingkungan, pengolahan air hujan atau air limbah secara biologis dan dikombinasikan dengan produksi oksigen, photobioreaktor lokal, perangkat biotech-based yang tidak menggunakan aliran listrik sebagai sumber energinya, atau bioprinting alga yang merupakan bioteknologi masa depan. Pada akhirnya, tujuan dari penerapan IoT dan bioteknologi ini adalah untuk memberikan kemajuan dan menciptakan kenyamanan lingkungan bagi masyarakat di kota cerdas hijau.

Sravani Challa, Mohammad Wazid, Ashok Kumar Das, Neeraj Kumar, Alavalapati Goutham Reddy, Eun-Jun Yoon, dan Kee-Young Yoo [10] pada makalahnya menjelaskan bahwa IoT menghasilkan manfaat ekonomi dengan mampu mengurangi keterlibatan manusia karena semua perangkatnya saling terhubung dan dapat diakses serta dikendalikan dari jarak jauh melalui jaringan internet sehingga meningkatkan akurasi, efisiensi, dan memudahkan kehidupan orang sehari-hari. Namun, IoT juga memiliki sifat heterogen dan dinamis sehingga membawa ancaman besar terhadap keamanan dan privasi. Seperti yang dapat dilihat pada gambar 1, dipertimbangkan empat skenario berbeda untuk model otentifikasi IoT yaitu Home, Transport, Community dan National. Keempat skenario tersebut memiliki perangkat pintar yaitu sensor dan aktuator yang memudahkan kehidupan orang sehari-hari dan saling terhubung melalui jaringan internet melalui gateway. Berbagai pengguna dapat mengakses perangkat IoT tersebut dengan saling menggunakan otentifikasi antara pengguna dengan perangkat melalui gateway. Oleh karena itu, salah satu persyaratan keamanan yang menjadi

tantangan di lingkungan IoT adalah otentifikasi, karena pengguna (pihak eksternal) secara langsung dapat mengakses informasi dari perangkat selama otentikasi terjadi antar pengguna dan perangkat yang diakses tersebut. Dalam makalahnya ini disajikan sebuah skema pembentukan kunci terotentifikasi berbasis signature yang bisa menjadi salah satu model iotentifikasi untuk aplikasi IoT di masa depan. Hal tersebut dikarenakan skema ini menggunakan bantuan logika BAN (Burrows-Abadi-Needham), keamanan skema dapat ditunjukkan secara informal dan formal menggunakan alat AVISPA, pengukuran berbagai parameternya dengan simulasi ketat menggunakan simulator NS2, dan ketiga teknik tersebut sudah dikenal luas dan banyak digunakan. Disebutkan juga bahwa skema yang diusulkan ini memiliki tingkat keamanan tinggi, efisien dalam komputasi dan biaya komunikasi, digabungkan dengan fitur fungsionalitas tambahan lainnya sehingga skema ini cocok untuk aplikasi praktis di lingkungan IoT dibandingkan skema terkait lainnya.

Liang Chen, Sarang Thombre, Kimmo Jarvinen, Elena Simona Lohan, Anette Alen-Savikko, Helena Leppakoski, M. Zahidul H. Bhuiyan, Shakila Bu-Pasha, Giorgia Nunzia Ferrara, Salomon Honkala, Jenna Lindqvist, Laura Ruotsalainen, Paivi Korpisaari, dan Heidi Kuusniemi [12] dalam artikel surveinya menyebutkan bahwa salah satu bagian terpenting dalam pertukaran informasi pada sistem IoT yang cerdas dan sadar konteks adalah informasi lokasi dengan fungsi penentuan posisi dan lokalisasi. Artikel ini melakukan survei sejauh mana solusi penanganan yang memadai dalam meningkatkan ketahanan, keamanan dan privasi layanan yang berbasis lokasi pada sistem IoT. Selain itu, dibahas juga tentang aspek keamanan dan privasi informasi lokasi berbasis IoT dari sudut pandang teknis dan hukum sehingga dapat memberikan rekomendasi untuk keamanan dan privasi informasi pada layanan IoT yang lebih kuat di masa depan. Solusi yang pertama disurvei adalah evaluasi terhadap ancaman dan solusi terkait sistem satelit navigasi global/ global navigation satellite system (GNSS) dan solusi berbasis non-GNSS. Solusi yang kedua adalah tentang solusi kriptografi. Dari berbagai surveinya dihasilkan banyak solusi yang tersedia untuk meningkatkan keamanan, ketahanan dan privasi layanan berbasis lokasi di IoT namun masih sering diiringi dengan biaya overhead yang signifikan dan memerlukan keahlian khusus dalam pengimplementasiannya sehingga masih banyak yang tidak menggunakan solusi-solusi tersebut. Selain itu juga ditemukan masalah dalam mengadaptasi solusi yang ada dengan framework IoT yang memiliki perangkat yang heterogen, masalah dalam mengamankan lokalisasi saat berhadapan dengan ancaman jahat yang kuat serta masalah pada sistem berbasis lokasi yang menjaga privasi. Harapan penulis artikel ini adalah untuk dapat membantu penelitian masa depan yang lebih berfokus pada IoT dengan sistem berbasis lokasi yang kuat, aman dan dapat menjaga privasi.

Arslan Munir, Prasanna Kansakar, dan Samee U. Khan [13] dalam makalahnya menyebutkan bahwa IoT adalah jaringan yang terdiri dari benda fisik, objek atau perangkat seperti tag identifikasi frekuensi radio, sensor, aktuator, dan komputer sehingga memungkinkan objek untuk dapat dirasakan dan dikendalikan dari jarak jauh dalam sebuah infrastruktur jaringan yang ada sehingga tercipta peluang integrasi dunia fisik ke dunia cyber secara langsung. IoT juga menjadi turunan dari cyberphysical systems (CPSs) dengan potensi objeknya dapat dikelompokkan ke dalam kluster geografis dan logis serta dapat menghasilkan data besar dari berbagai lokasi sehingga dibutuhkan pemrosesan data yang lebih efisien. Cloud Computing merupakan komputasi berbasi internet yang menyediakan sumber daya yang dapat diakses dan dikonfigurasi secara bersama-sama sesuai permintaan. Komputasi ini mampu menangani jumlah data yang besar, namun tantangan hadir ketika dibutuhkan transfer data dari dan ke komputer cloud dengan bandwidht terbatas. Akibatnya, muncul kebutuhan terhadap komputasi yang dapat dilakukan di dekat sumber data. Fog Computing menjadi salah solusi tantangan tersebut. Fog Computing merupakan tren baru dalam memproses data di dekat lokasi sumber data yang mendorong jauh aplikasi, layanan, data, daya komputasi dan pengambilan keputusan dari the centralized nodes menjadi the logical extremes dari sebuah jaringan sehingga memungkinkan analisis dan pengolahan data dilakukan di sumber data serta secara signifikan dapat mengurangi volume data yang harus ditransfer antar perangkat akhir dan cloud. Selain itu akurasi data per lokasi dapat dicapai dengan baik dibandingkan menggunkan cloud. Meskipun fog computing dapat menjadi solusi tantangan tersebut diatas, namun akan memunculkan masalah lain seperti kinerja contemporary fog nodes, hasil, energi dan kendala latensi yang tidak dapat memenuhi harapan awal dari aplikasi IoT di masa depan kecuali arsitekturnya disesuaikan dengan persyaratan aplikasi ini. Artikel ini memiliki tujuan untuk mengatasi tantangan arsitektur aplikasi IoT/CPSs di masa depan

dengan memanfaatkan fog computing. Adapun kontribusi utama yang disebutkan di makalah ini adalah sebagai berikut:

- Paradigma arsitektur IoT yang merupakan integrasi antara Cloud dan Fog Computing dalam archetype yang terpadu. Arsitektur IFCIoT yang menjanjikan peningkatan kinerja, efisiensi energi dan waktu respons, skalabilitas dan akurasi lokal yang lenih baik pada aplikasi IoT/CPS di masa depan.
- Usulan arsitektur edge-server berlapis yang hemat energi. Arsitektur ini meliputi aplikasi, analitik, virtualisasi, konfigurasi ulang, dan hardware layers yang memfasilitasi abstraksi dan implementasi fog computing dimana berbagai layanan, aplikasi, data dan penyedia konten saling terlibat.
- Diskusi tentang fog computing yang menjadi pendorong utama dalam sistem transportasi cerdas / intelligent transportation systems (ITSs) di masa yang akan datang dengan memetakan usulan arsitektur fog yang adaptif dan dapat dikonfigurasi ulang.
- Aplikasi potensial lainnya yang dapat menggunakan arsitektur IFCIoT sepert kota pintar, lingkungan pintar, serta analisis dan kontrol data yang dilakukan secara realtime dibidang pertanian.

Makalah ini [13] juga membahas tentang perbedaan antara fog, cloud dan edge computing. Dengan mengambil kesimpulan dari beberapa definisi fog computing, pemakalah menyimpulkan bahwa fog computing adalah perluasan dari paradigma cloud computing tradisional ke edge dari suatu jaringan sehingga memungkinkan pembuatan aplikasi atau layanan yang lebih baik lagi. Singkatnya, Fog adalah paradigma edge computing dan Micro Data Center 9MDC) untuk IoT dan jaringan sensor nirkabel (WSN). Kesimpulan utama dari makalah ini menjelaskan bahwa fog computing memiliki berbagai keunggulan dibandingkan cloud computing untuk aplikasi yang membutuhkan waktu pemrosesan yang lebih cepat dengan mengurangi latensi dan delay jitter, responsif cepat, memberikan dukungan mobilitas dan kostumisasi berbasis lokasi. Meskipun demikian, fog computing bukanlah pengganti cloud computing karena beberapa fungsi cloud computing masih diperlukan. IoT di masa depan akan dapat diwujudkan dengan mensinergikan fog dan cloud computing.

Parisa Ramezani dan Abbas Jamalipour [14] dalam makalahnya menyebutkan bahwa kelangkaan energi merupakan salah satu tantangan yang harus diatasi dalam mengadopsi paradigma IoT secara luas. Dibutuhkan sebuah langkah kunci yang dapat merealisasikan jaringan IoT yang mandiri dan dapat menyediakan energi sendiri. Seiring dengan berjalannya waktu, muncul solusi terhadap kelangkaan energi yaitu energy harvesting atau pemanenan energi yang dapat menjawab kekhawatiran atas keterbatasan energi. Salah satu metode pemenenan energi yang menarik banyak peneliti karena keunggulannya yang jelas adalah pemanenan energi RF dan memunculkan jaringan komunikasi bertenaga nirkabel atau bisa disebut wireless powered communication networks (WPCNs). WPCs memungkinkan pengguna yang memiliki keterbatasan energi mendapatkan alternatif lain dari transfer energi nirkabel pada energi terintegrasi dan jalur akses informasi yang disebut dengan hybrid access point (HAP). Makalah ini juga akan meninjau dan membahas penelitian lebih lanjut yang dilakukan di bidang WPCN. Disajikan pula beberapa poin untuk WPCN yang harus diperhitungkan agar dapat beroperasi dengan sempurna di lingkungan IoT. WPCN merupakan salah satu langkah kunci menuju realisasi jaringan IoT yang mandiri energi yang sebelumnya harus eslalu berkompromi dengan Quality of Services (QoS) dan konsumsi energi di setiap transfernya. Ada literatur terbaru tentang WPCN yang merupakan upaya peningkatan kinerja dari jaringan IoT ini. Meskipun WPCN menjanjikan atribut yang diharapkan, namun karena masih dalam tahap awal maka penelitian lebih lanjut harus terus dilakukan untuk penggunaan WPCN ke dalam lingkungan IoT di masa depan. Salah satunya adalah masalah keamanan yang merupakan masalah penting yang harus diperhatikan secara serius saat merancang WPCN, karena mekanisme keamanan yang kompleks mengakibatkan konsumsi energi dalam jumlah besar sehingga tidak cocok untuk perangkat bertenaga nirkabel yang memiliki keterbatasan energi. Namun di masa depan akan tiba saatnya penggunaan sistem yang berbeda untuk maksud dan tujuan yang berbeda harus diantisipasi dan skema alokasi sumber daya harus ditinjau kembali dengan mempertimbangkan keamanan saat berdampingan dengan IoT. Contohnya pada WPCN konvensional, diharapkan adanya peningkatanan energi yang dipanen sehingga dapat meningkatkan daya pancar dan

hasil. Namun, hal tersebut memungkinkan perangkat untuk mentransmisikan data dengan daya tinggi sehingga memudahkan calon penyadap untuk dapat mendengan informasi yang dikirim tersebut. Dalam kasus teresbut, sebenarnya kalau pertimbangan keamanan diabaikan maka alokasi waktu dan daya dapat secara optimal digunakan untuk transfer energi dan informasi. Singkatnya, integrasi WPCN ke dalam lingkungan IoT membutuhkan solusi yang dapat mengkombinasikan antara strategi serta teknik baru sehingga dapat memenuhi kebutuhan jaringan IoT di masa depan.

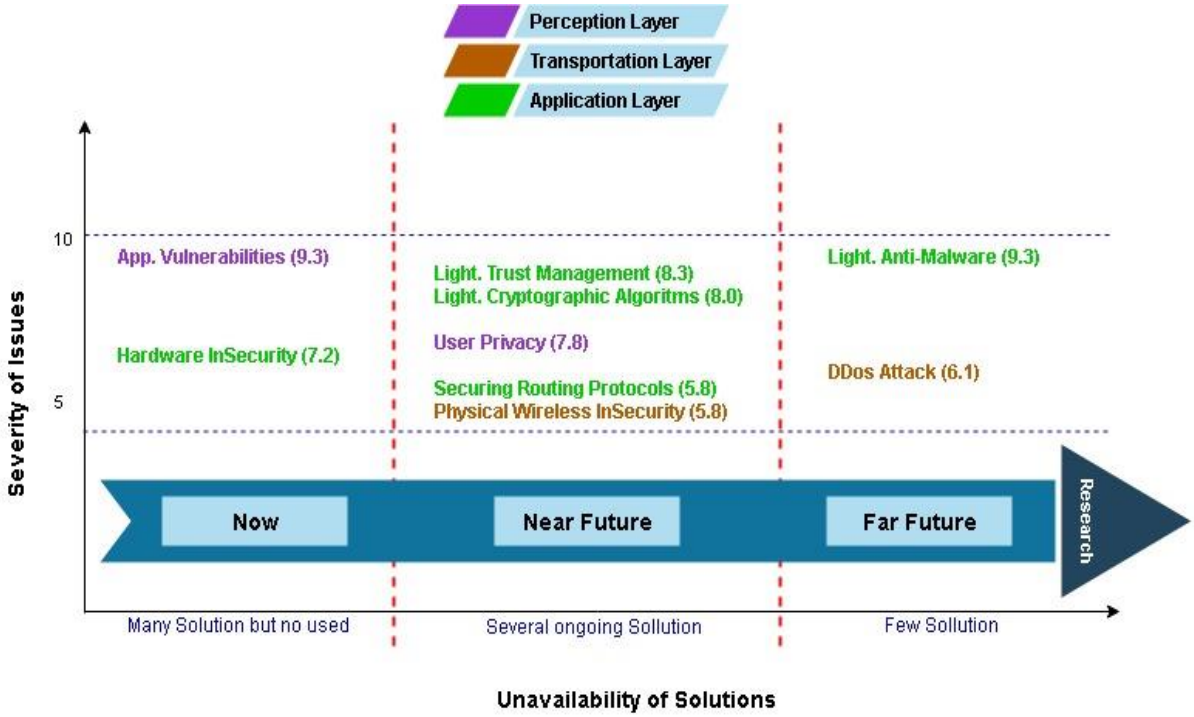
Sama seperti pada artikel-artikel sebelumnya, Joshua E. Siegel, Sumeet Kumar, dan Sanjay E. Sarma [15] dalam makalahnya juga menyebutkan bahwa penggunaan sumber daya serta kehawatiran tentang privasi dan keamanan menyebabkan terbatasnya pertumbuhan IoT. Namun makalah ini juga mengusulkan solusi untuk memanfaatkan sumber daya cloud untuk memfasilitasi IoT pada perangkat terbatas yang dimodelkan pada penggunaan konteks dan kognisi oleh manusia sehingga dapat meningkatkan keamanan dan efisiensi. Arsitektur yang dihadirkan ini menerapkan proses pengetahuan yang dapat memberikan keamanan melalui abstraksi dan privasi melalui fusi data jarak jauh dengan menguraikan lima elemen arsitektur dan pertimbangan konsep kunci "Data Proxy" dan "Cognitive Layer". Data Proxy menggunakan sistem yang dimodelkan secara digital sehingga mencerminkan objek dengan data input dan penggunaan sumber daya seminimal mungkin tapi sensor sistem tetap dapat memenuhi target kualitas data. Cognitive Layer menerapkan model pemantauan evolusi sistem dan menstimulasikan dampak sebelum eksekusi. Menurut makalah ini juga disebutkan adanya peluang arsitektur ini dalam mengurangi hambatan teknis, ekonomi dan sentimen untuk adopsi IoT di masa depan. Adapun beberapa peluang yang diidentifikasi di makalah ini adalah usulan tentang penciptaan arsitektur baru dengan target Quality of Data (QoD), lapisan keamanan dan kognitif, proxy data dengan pemodelan berbasis matematika, pengoptimalan biaya mengambilan data dan meminimalkan kesalahan untuk meningkatkan IoT.

Hampir sama dengan makalah sebelumnya, pemakalah Mario Frustaci, Pasquale Pace, Gianluca Aloi, dan Giancarlo Fortino [16] menyebutkan tentang masalah keamanan dan privasi yang merupakan tantangan besar bagi IoT. Namun tantangan tersebut juga dapat menjadi faktor pendukung dalam menciptakan "trust ecosystem". Makalah ini berfokus pada Social Internet of Things atau SIoT yang merupakan paradigma baru dimana IoT digabungkan dengan jejaring sosial yang memungkinkan orang dan perangkat untuk dapat saling berinteraksi dan memfasilitasi pertukaran informasi. Perkembangan cyber threats disebabkan oleh kerentanan intrinsik antara perangkat IoT dengan keterbatasan sumber daya dan teknologi yang heterogen beserta kurangnya desain khusus standara IoT. Ada perspektif tiga lapisan utama dari model sistem IoT yang dicoba untuk dianalisis secara taksonomi yaitu:

- Perception Layer merupakan lapisan pertama yang mencakup sensor dan aktuator serta merupakan sensor IoT fisik yang mendukung pengukuran, pengumpulan dan pemrosesan data. Ancaman keamanan utama pada lapisan ini disebabkan oleh keterbatasan sumber daya dan struktur yang ditata secara terdistribusi. Adapun ancaman yang berasal dari lapisan ini diantaranya adalah Physical Attacks seperti Node Tampering dan Malicious Code Injection, Impersonation, Denial of Service (DoS) Attacks, Routing Attacks, dan Data Transit Attacks.
- Transportation Layer merupakan lapisan yang menyediakan akses ke seluruh jaringan melalui jaringan komunikasi seperti 3G, WiFi, jaringan ad hoc, dan sebagainya untuk mengirimkan informasi yang dikumpulkan oleh perception layer ke sistem pemrosesan informasi tertentu. Ancaman pada jaringan LTE berbasis IP yang memiliki arsitektur terbuka dan heterogen lebih banyak dibandingkan yang menggunakan jaringan 3G. Adapun ancaman utama pada lapisan ini yaitu Routing Attacks, DoS Attacks, dan Data Transit Attacks.
- Application Layer merupakan lapisan yang menyediakan layanan sesuai permintaan pengguna sehingga harus memiliki kemampuan untuk menyediakan layanan pintar kerkualitas tinggi dan dapat memenuhi kebutuhan pengguna. Ancaman utama pada lapisan ini adalah Data Leakage, DoS Attack, dan Malicious Code Injection.

Dari ketiga perspektif diatas, pemakalah menyimpulkan bahwa tingkat paling rentan adalah pada lapisan pertama yaitu Perception Layer karena sifat fisik perangkat IoT yang masih terbatas dalam hal sumber daya dan teknologi heterogennya.

Pada gambar 2 dapat dilihat analisis lanjutan yang dilakukan terkait arah penelitian dari ketiga perspektif lapisan sehingga dapat dilakukan pertimbangan berikut ini.



Gambar 2. Arah penelitian (adaptasi dari [16])

- Ketidakamanan perangkat keras serta kerentanan aplikasi pada umumnya sudah memiliki banyak pilihan solusi yang dapat diambil. Namun pengimplementasiannya masih bergantung pada produsen perangkat atau pengembang perangkat lunak.
- Masih kurangnya anti-malware ringan dan serangan DDos. Meskipun sudah ada beberapa solusi, namun memiliki indeks keparahan menengah-tinggi.
- Beberapa solusi masalah kemananan sudah mulai berjalan namun masih belum matang.

Dari pertimbangan diatas, disimpulkan bahwa penelitian selanjutnya harus berkonsentrasi pada pemecahan masalah kritis dengan menyediakan solusi berkelanjutan yang semakin layak dengan kemajuan teknologi.

Pada makalah sebelumnya, disebutkan berbagai macam perkembangan IoT di masa depan berikut ancaman utama dalam penerapannya di kehidupan sehari-hari. Ancaman tersebut tentulah tidak bisa dilepaskan dari kejahatan digital dan berhubungan dengan bagaimana jejak kejahatan digital dapat dikumpulkan sebagai bukti di pengadilan dengan menggunakan forensik digital. Hubungannya dengan IoT adalah di masa yang akan datang penggunaan IoT juga akan diterapkan dalam pengumpulan data forensik digital seperti yang disebutkan oleh pemakalah Luca Caviglione, Steffen Wendzel, dan Wojciech Mazurczyk [17]. Karena penggunaan IoT dapat menciptakan interaksi antara dunia maya (cyber) dan dunia nyata maka Digital IoT Forensics adalah sebuah cara yang efektif untuk mengumpulkan data dan informasi tentang lingkungan nondigital. Contohnya node IoT yang dapat memberikan bukti apakah seseorang hadir disuatu tempat atau ruangan baik lokasi dan waktu terekam jelas dengan menginvestigasi sensor kehadiran in-door meskipun tidak hanya satu orang yang dapat memicu sensor kehadiran tersebut dan terkait juga dengan masalah privasi. Karena perangkat pribadi, peralatan maupun node IoT dapat membalikan nasib seseorang di persidangan, maka makalah ini memfokuskan pada bagaimana pengaruh IoT dan cyber-physical system (CPS) terhadap forensik digital, baik dalam hal tantangan maupun peluangnya di masa yang akan datang.

Penyebaran IoT dan cyber-physical system (CPS) begitu signifikan dan penggunaannya yang meningkat baik untuk liburan maupun automasi rumah (domotik), IoT juga merupakan inti dari revolusi industri 4.0 sehingga mendapatkan perhatian khusus dari para penjahat cyber, pakar keamanan, penegak hukum atau law enforcement agencies (LEA) dan para profesional lainnya yang berhubungan dengan forensik digital. Framework IoT dan CPS banyak memberikan keuntungan karena optimasinya di berbagai proses manufaktur, namun hal tersebut juga menciptakan peluang baru untuk ancaman dan serangan adhoc seperti spionase industri atau cybersabotage. Dengan menyelidiki komponen IoT dan CPS baik pada skenario kecil maupun besar, diharapkan dapat dikumpulkan data sebagai bukti dalam forensik digital untuk selanjutnya akan dilakukan analisis serangan pada perangkat IoT serta investigasi kejahatan yang membantunya di dunia fisik. Perangkat IoT memiliki peralatan untuk mengontrol dan memantau serta sejumlah sensor dan aktuator, namun data historis dan status aktuator tidak selalu persisten dan dapat diakses oleh penyidik sehingga mengakibatkan lingkungan IoT menjadi sangat berbeda dari jaringan klasik dan penyebaran komputasi. Hal tersebut menjadi sebuah tantangan baru baik di bidang forensik digital maupun teknologi IoT, termasuk masalah berikut:

- Rekaman persisten yang sulit diakses disebabkan oleh kendala sumber daya, keterbatasan memori dan kinerja komputasi pada skenario IoT.

- Kesulitan mengakses nilai yang disimpan pada perangkat IoT yang disebabkan oleh penyebaran perangkat IoT dengan antar muka berpemilik sehingga penyidik perlu melakukan upaya rekayasa balik yang tidak dapat diabaikan.

- Keterbatasan energi juga berpengaruh pada seringnya informasi yang dikirim menjadi terputus-putus atau tidak lengkap.

Masih belum jelas bagaimana perangkat IoT dapat diinvestigasi secara baik dalam sudut pandang analisis biaya-manfaat. Biaya yang disebutkan disini dapat bersifat yuridis, teknis, atau ekonomis. Selain itu, terdapat perbedaan tipe IoT, aksesibilitas, antarmuka, fitur khusus vendor dan strategi penyimpanan data pada masing-masing perangkat IoT sehingga setiap perangkat IoT, lokasi, jenis dan atribut aksesibilitasnya harus difahami dan dipertimbangkan masing-masingnya untuk investigasi forensik. Ada juga perangkat IoT yang sering berpindah lokasi sehingga menjadi tantangan menarik untuk dapat mengaksesnya. Tabel 1 merangkum bagaimana properti perangkat IoT dan CPS dapat mempengaruhi penyelidikan disertai tantangan yang akan dihadapi saat penerapannya.

TABLE I. PROPERTI INTERNET OF THINGS DAN PERANGKAT SISTEM FISIK CYBER DAN PENGARUHNYA TERHADAP FORENSIK DIGITAL MODERN. (ADAPTASI DARI [17])

Property	**Relation to (digital) forensic investigation**	**Exemplary challenges**
Density of device Deployment	Mempengaruhi resolusi peristiwa yang terjadi di lingkungan fisik.	Merekonstruksi peristiwa fisik berdasarkan perangkat yang digunakan tidak merata (misalnya, tidak semua ruang memiliki kepadatan yang sama dari simpul dan informasi Internet of Things [IoT]). Ini juga dapat bervariasi sesuai dengan lingkungan yang dipertimbangkan.
Device type	Menpengaruhi jenis data atau informasi	Penyediaan kerangka kerja berbantuan komputer, berbasis bukti, dan bukti pengadilan untuk rekonstruksi peristiwa. Perangkat lunak seperti itu harus dapat memperhitungkan seperangkat perangkat campuran / meningkat, misalnya dengan menggunakan arsitektur plug-in.
Device location	Mempengaruhi aksesibilitas fisik perangkat untuk penyelidikan forensik digital (perangkat mungkin ditempatkan di belakang batas negara) dan mempengaruhi area lingkungan fisik mana yang dicakup oleh perangkat tersebut (bagian dari situs forensik yang telah dipengaruhi).	Kembangkan analisis biaya-manfaat untuk menentukan apakah perangkat IoT yang terletak di area yang sulit dijangkau layak diakses. Satu ide adalah menggunakan basis data yang menunjukkan properti perangkat yang berguna untuk investigasi forensik dan detail tambahan seperti keakuratan sensor onboard.
Recording history	Semua informasi yang tersedia pada perangkat IoT dapat direkam secara lokal atau di cloud. Penyimpanan lokal biasanya terbatas; dengan demikian, jumlah nilai sensor / aktuator yang direkam disimpan di bawah ambang tertentu. Data yang lebih lama mungkin tidak dapat diakses.	Integrasi otomatis perangkat IoT ke dalam proses rekonstruksi peristiwa fisik. Ini membutuhkan pengambilan sejarah perekaman sensor dan menempatkannya dengan benar dalam kerangka waktu acara yang akan direkonstruksi. Ini bisa memerlukan dukungan alat analitik visual yang mampu menangani perangkat yang menyediakan data dengan waktu dan posisi spasial yang tidak konsisten atau tidak akurat.
Device interfaces	Antarmuka yang digunakan untuk mengakses bukti sangat mempengaruhi jumlah	Penyediaan metainterface terpadu untuk forensik IoT yang mencakup spektrum besar perangkat yang berbeda dan antarmuka tingkat

Property	Relation to (digital) forensic investigation	Exemplary challenges
	informasi yang dapat diambil. Beberapa jenis informasi mungkin tidak disediakan oleh antarmuka tertentu sementara yang lain. Dalam beberapa kasus, antarmuka mungkin tidak berdokumen oleh vendor.	rendah dari beberapa vendor. Ini kemungkinan dapat ditangani secara memadai oleh proyek-proyek komunitas yang lebih besar.

III. ANALYSIS OF THE GAPS AND OPPORTUNITIES

Sejauh ini, makalah-makalah yang telah di survei kebanyakan berfokus pada penggunaan IoT di masa yang akan datang dalam berbagai bidang disertai tantangan dan ancaman yang muncul dari penerapannya sehingga banyak penelitian yang dilakukan dalam mencari solusi dari tantangan dan ancaman tersebut. Banyak keuntungan yang didapatkan dari penerapan IoT di kehidupan sehari-hari. Selain mempermudah pekerjaan baik dalam mengontrol maupun memonitor suatu perangkat, juga memberikan nilai ekonomis.

Berbagai bidang keilmuan sudah mulai diperkenalkan dengan teknologi IoT. Penerapannya membuka peluang baru bahkan keilmuan baru yang bermanfaat bagi manusia secara keseluruhan. Penerapan IoT sudah mulai banyak dilakukan, baik dalam skala kecil seperti mengontrol pendingin udara, maupun dalam skala besar seperti kota pintar, pabrik pintar, kampus pintar dan sebagainya.

IV. CONCLUSION

Dimasa yang akan datang, IoT akan menjadi bagian yang tidak terpisahkan dari kehidupan sehari-hari. Dimulai dengan muncul berbagai ide penggunaan teknologi IoT pada perangkat yang terkait kebutuhan atau aktifitas masyarakat saat ini. Namun selain manfaat yang dihasilkan oleh perangkat IoT, terdapat ancaman yang menyertai penerapannya seperti kejahatan cyber. Sudah banyak dilakukan penelitian untuk bisa mendapatkan solusi yang tepat dari berbagai tantangan dan ancaman yang mungkin terjadi. Selain tantangan dan ancaman yang muncul dari penerapan IoT, pengembangan dalam penggunaan IoT juga menjadi fokus penelitian.

REFERENCES

[1] S.R.Vijayalakshmi, S.Muruganand, "A survey of Internet of Things in fire detection and fire industries", International conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), India, 2017.

[2] Recommendation ITU-T Y.2060, “Overview of Internet of Thing”, (06/2012).

[3] Michele Zorzi, Alexander Gluhak, Sebastian Lange, Alessandro Bassi, "From Today’s Intranet Of Things To A Future Internet Of Things: A Wireless- And Mobility-Related View", IEEE Wireless Communications Volume: 17, Issue: 6, December 2010.

[4] Huansheng Ning, Ziou Wang, "Future Internet of Things Architecture: Like Mankind Neural System or Social Organization Framework?", IEEE Communications Letters, vol. 15, no. 4, april 2011.

[5] Muhammad S. Khan, Mohammad S. Islam, Hai Deng, "Design of a Reconfigurable RFID Sensing Tag as a Generic Sensing Platform Toward the Future Internet of Things", IEEE Internet Of Things Journal, vol. 1, no. 4, august 2014

[6] Kazi Masudul Alam, Mukesh Saini, Abdulmotaleb El Saddik, "Toward Social Internet of Vehicles: Concept, Architecture, and Applications", IEEE Access The Journal for rapid open access publishing, volume 3, 2015.

[7] Dejan Vukobratovic, Dusan Jakovetic, Vitaly Skachek, Dragana Bajovic, Dino Sejdinovic, Güne Karabulut Kurt, Camilla Hollanti, Ingo Fischer, "CONDENSE: A Reconfigurable Knowledge Acquisition Architecture for Future 5G IoT", IEEE Access Special Section On Internet Of Things (IoT) In 5G Wireless Communications, volume 4, 2016.

[8] Bill Montgomery, "Future Shock, IoT benefits beyond traffic and lighting energy optimization", IEEE Consumer Electronics Magazine, 2015.

[9] Pavel M. Gotovtsev, Andrey V. Dyakov, "Biotechnology and Internet of Things for Green Smart City Application", IEEE 3rd World Forum on Internet of Things (WF-IoT), Reston, VA, USA, 2016.

[10] Sravani Challa, Mohammad Wazid, Ashok Kumar Das, Neeraj Kumar, Alavalapati Goutham Reddy, Eun-Jun Yoon, Kee-Young Yoo, "Secure Signature-Based Authenticated Key Establishment Scheme for Future IoT Applications", IEEE Access, volume 5, 2017.

[11] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions," Future Generat. Comput. Syst., vol. 29, no. 7, pp. 1645-1660, 2013.

[12] Liang Chen, Sarang Thombre, Kimmo Jarvinen, Elena Simona Lohan, Anette Alen-Savikko, Helena Leppakoski, M. Zahidul H. Bhuiyan, Shakila Bu-Pasha, Giorgia Nunzia Ferrara, Salomon Honkala, Jenna Lindqvist, Laura Ruotsalainen, Paivi Korpisaari, Heidi Kuusniemi, "Robustness, Security and Privacy in Location-Based Services for Future IoT: A Survey", IEEE Access Special Section On Security And Privacy In Applications And Services For Future Internet Of Things, Volume 5, 2017.

[13] Arslan Munir, Prasanna Kansakar, Samee U. Khan, "IFCIoT: Integrated Fog Cloud IoT. A novel architectural paradigm for the future Internet of Things." IEEE Consumer Electronics Magazine, volume 6, 2017.

[14] Parisa Ramezani, Abbas Jamalipour, "Toward the Evolution of Wireless Powered Communication Networks for the Future Internet of Things", IEEE Network, volume 31, 2017.

[15] Joshua E. Siegel, Sumeet Kumar, Sanjay E. Sarma," The Future Internet of Things: Secure, Efficient, and Model-Based", IEEE Internet Of Things Journal, vol. 5, no. 4, 2018.

[16] Mario Frustaci, Pasquale Pace, Gianluca Aloi, Giancarlo Fortino, " Evaluating Critical Security Issues of the IoT World: Present and Future Challenges", IEEE internet of things journal, vol. 5, no. 4, 2018.

[17] Luca Caviglione, Steffen Wendzel, Wojciech Mazurczyk, "The Future of Digital Forensics: Challenges and the Road Ahead", IEEE Security & Privacy, Volume: 15 , Issue: 6, 2017.