Tinjauan Ancaman dan Solusi Keamanan pada Teknologi *Internet of Things*

(*Review on Security Threat and Solution of Internet of Things Technology*)

Warsun Najib[1], Selo Sulistyo[2], Widyawan[3]

***Abstract*—Internet of Things (IoT) is a well-known technology globally, which helps to connect things such as sensors, vehicles, hospital-instruments, industries, and consumer-goods through the internet. Compact smart devices constitute an essential part of IoT. They range widely in use, size, computing resources, and memory. However, integrating these intelligent things into the internet introduces several security challenges, because most internet technologies and communication protocols were not designed specifically to support IoT. Moreover, IoT's commercialization has led to public security concerns, including personal privacy issues, threats of cyberattacks, and organized crime. This review aims to provide a comprehensive list of IoT vulnerabilities and counter-measures against them. To achieve this goal, we first describe three widely-known IoT reference models and define security in the context of IoT. Second, we discuss the potential motivations of the attackers who target this technology. Third, we discuss different attacks and threats. Fourth, we describe possible countermeasures against these attacks. Finally, we describe emerging security challenges in IoT system.**

***Intisari*—*Internet of Things* (IoT) adalah teknologi yang sangat populer akhir-akhir ini di seluruh dunia, yang membantu menghubungkan objek-objek seperti sensor, kendaraan, instrumen rumah sakit, industri, dan peralatan rumah tangga melalui internet. Perangkat pintar yang ringkas merupakan bagian penting dari IoT. Perangkat ini beragam dalam penggunaan, ukuran, sumber daya komputasi, dan memori. Namun, pengintegrasian peranti-peranti cerdas ini ke dalam jaringan internet memunculkan berbagai tantangan keamanan karena mayoritas teknologi internet dan protokol komunikasi tidak dirancang secara khusus untuk mendukung peranti IoT. Selain itu, komersialisasi IoT telah menyebabkan masalah keamanan, termasuk masalah privasi, ancaman serangan dunia maya, dan kejahatan terorganisasi. Untuk memberikan pedoman bagi pihak-pihak yang ingin mengembangkan keamanan IoT dan berkontribusi pada peningkatannya, survei ini berupaya memberikan daftar kerentanan dan penanggulangan secara komprehensif terhadap ancaman-ancaman tadi. Untuk mencapai tujuan ini, pertama-tama dipaparkan tiga model referensi IoT yang dikenal luas dan mendefinisikan keamanan dalam konteks IoT. Kedua, dibahas kemungkinan penerapan IoT pada berbagai bidang dan potensi serta motivasi para penyerang yang menargetkan teknologi IoT ini. Ketiga, dilakukan identifikasi dan klasifikasi berbagai serangan dan ancaman IoT. Keempat, dideskripsikan metode penanggulangan terhadap serangan IoT. Pada bagian akhir, diperkenalkan dua tantangan keamanan IoT yang muncul yang belum dijelaskan secara rinci dalam publikasi sebelumnya.**

***Kata Kunci*—*Internet of Things, Security, Security Solution, IoT Security, Threats*.**

[1,2,3] *Departemen Teknik Elektro dan Teknologi Informasi, Universitas Gadjah Mada, Jalan Grafika 2. Yogyakarta 55281 INDONESIA (telp: 0274-552305; e-mail: warsun@ugm.ac.id)*

I. PENDAHULUAN

Teknologi *Internet of Things* (IoT) pertama kali diperkenalkan oleh Kevin Ashton pada tahun 1999. Konsep IoT diartikan sebagai sebuah kemampuan untuk menghubungkan objek-objek cerdas dan memungkinkannya untuk berinteraksi dengan objek lain, dengan lingkungan, maupun dengan peralatan komputasi cerdas lainnya melalui jaringan internet [1]. IoT dalam berbagai bentuknya telah mulai diaplikasikan pada banyak aspek kehidupan manusia. Meluasnya adopsi berbagai teknologi IoT membuat kehidupan manusia menjadi jauh lebih mudah dan nyaman. Dari sisi pengguna perorangan, IoT sangat terasa pengaruhnya dalam bidang domestik, seperti pada aplikasi rumah dan mobil cerdas. Dari sisi pengguna bisnis, IoT sangat berpengaruh dalam meningkatkan jumlah produksi, efisiensi, kualitas produksi, pemantauan distribusi barang, mencegah pemalsuan, mempercepat waktu ketersediaan barang pada pasar retail, manajemen rantai pasok, dan sebagainya.

Proyek Casagras mendefinisikan IoT sebagai sebuah infrastruktur jaringan global yang menghubungkan benda-benda fisik dan virtual melalui proses akuisisi data dan kemampuan komunikasi. Infrastruktur ini mencakup jaringan internet yang telah ada dan juga pengembangannya. Semua ini akan menawarkan identifikasi objek, sensor, dan kemampuan koneksi sebagai dasar untuk pengembangan layanan (*service*) dan aplikasi yang independen. IoT juga ditandai dengan tingkat otonom yang tinggi untuk proses-proses akuisisi data, pertukaran *event*, konektivitas jaringan, dan interoperabilitas [2]. Organisasi *European Technology* Platform *on Smart System* mendefinisikan IoT sebagai jaringan yang dibentuk oleh benda-benda atau objek-objek yang memiliki identitas dan properti virtual yang beroperasi di ruang pintar menggunakan antarmuka cerdas untuk terhubung dan berkomunikasi dengan pengguna, konteks sosial, dan lingkungan [3].

Makalah ini mengambil fokus pada survei tentang berbagai ancaman keamanan pada teknologi IoT dan alternatif solusinya. Setelah pendahuluan, pada bagian II dipaparkan berbagai jenis aplikasi IoT, sedangkan bagian III mendiskusikan arsitektur IoT. Bagian IV merangkum berbagai jenis ancaman keamanan IoT, sedangkan solusi keamanan didiskusikan pada bagian V. Bagian VI memaparkan tantangan keamanan baru pada IoT dan diakhiri dengan bagian VII yaitu kesimpulan.

II. Jenis Aplikasi *Internet of Things*

Beragam aplikasi IoT telah banyak dibuat prototipe dan juga implementasinya, seperti aplikasi-aplikasi *smart-building*, *smart-home*, *smart-vehicle*, *smart-farming*, dan *smart-industry*. Pada bagian ini dibahas karakteristik dari beberapa sistem IoT yang telah banyak diimplementasikan di kehidupan sehari-hari.

A. Aplikasi Smart Vehicle

Aplikasi *smart-vehicle* atau kendaraan cerdas merupakan pengembangan dari sistem transportasi tradisional dengan menambahkan fitur-fitur cerdas pada komponen kendaraan. Dengan aplikasi IoT, pemilik kendaraan dapat mengunci ataupun membuka kunci secara *remote*, mengunduh peta jalan, mengakses layanan navigasi, dan mengakses informasi trafik. Selain itu, mobil yang terkoneksi internet dapat dilengkapi fitur keamanan agar terlindung dari pencurian kendaraan.

B. Aplikasi Smart Building

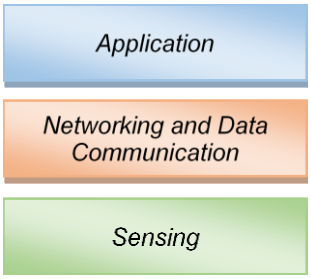
Rumah dan bangunan cerdas memungkinkan sistem pengelolaan energi secara efisien. Sebagai contoh, sistem pengatur suhu yang dilengkapi dengan sensor suhu dan algoritme analisis data dapat melakukan pengaturan terhadap suhu udara ruangan berdasarkan preferensi dan kebiasaan pengguna. Pengendali cerdas lainnya dapat mengatur kecerahan lampu berdasar aktivitas pengguna. Berbagai perabot rumah tangga, seperti kulkas, televisi, dan sistem keamanan, dapat memiliki unit pengolahan masing-masing dan menyediakan akses via internet. Peranti-peranti cerdas ini akan meningkatkan kenyamanan pengguna. Peranti yang dapat dikendalikan dari jauh ini akan menerima perintah dari pengguna untuk melakukan suatu aksi pengaturan yang akan memberikan efek pada lingkungan di sekitarnya. Dengan demikian, serangan yang terjadi pada perangkat ini akan dapat menyebabkan dampak fisik pula [4].

C. Pemantauan Kesehatan

Perkembangan terbaru pada bidang *biomedical*, pengolahan isyarat, peranti hemat energi, dan komunikasi nirkabel telah merevolusi teknologi kesehatan. Adaptasi teknologi IoT pada bidang kesehatan ini mencakup pemantauan kesehatan pribadi, sistem pemberian obat, pengambilan data pasien jarak jauh, dan sebagainya. Data-data dari sensor yang dipakai oleh pasien diakuisisi kemudian diolah dan disimpan dalam jangka panjang sehingga dapat digunakan untuk rekam medis berkelanjutan [5]. Berbagai macam sensor cerdas telah dipakai pada alat-alat *fitness*, diet, dan sistem pemantau kesehatan [6]. Masa depan sistem IoT pada bidang kesehatan mengarah pada perancangan pemantau kesehatan personal yang memungkinkan deteksi dini suatu penyakit.

D. Manajemen Energi

Penggunaan sistem cerdas pada bidang energi berbasis IoT yang mengintegrasikan sensor dan aktuator tertanam (*embedded*) memungkinkan pendekatan proaktif untuk mengoptimalkan konsumsi energi. Misalnya sistem cerdas pada stopkontak, lampu, kulkas, dan televisi cerdas yang dapat dikontrol secara *remote* diharapkan dapat berbagi informasi kepada perusahaan pemasok energi listrik untuk melakukan optimasi konsumsi energi di rumah cerdas tersebut. Fitur tambahan lainnya memungkinkan pengguna untuk melakukan penjadwalan yang pada akhirnya dapat menghemat penggunaan energi listrik.



Gbr. 1 Model arsitektur IoT tiga *layer*.

E. Manajemen Konstruksi

Pemantauan dan pengelolaan infrastruktur modern, seperti jembatan, lampu lalu lintas, rel kereta, dan gedung, merupakan salah satu aplikasi sistem IoT [7]. IoT dapat digunakan untuk memantau perubahan mendadak dari kondisi struktural yang dapat berdampak pada keselamatan dan risiko keamanan. Sistem IoT juga memungkinkan perusahaan konstruksi untuk membagi informasi tentang rancangan dan desain yang dimiliki. Sebagai contoh, perusahaan konstruksi dapat membagi informasi perbaikan jalan kepada perusahaan navigasi berbasis *Global Positioning System* (GPS). Berdasarkan informasi tersebut, peranti GPS dapat menentukan rute alternatif untuk menghindari jalan yang sedang dalam perbaikan.

F. Pemantauan Lingkungan

Penggunaan objek-objek cerdas yang dilengkapi sensor memungkinkan pemantauan lingkungan, termasuk di dalamnya pendeteksian situasi darurat, seperti banjir yang memerlukan operasi tanggap darurat. Selain itu, kualitas udara dan air dapat diteliti dengan peranti dan sensor berbasis IoT. Kelembapan udara dan temperatur juga dapat dengan mudah dipantau dengan sistem IoT [8].

III. Model Arsitektur *Internet of Things*

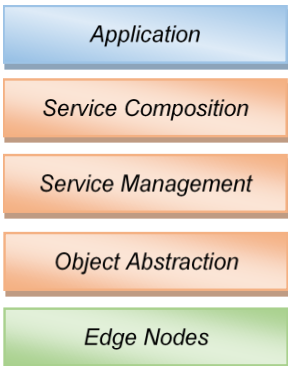
Ada tiga model arsitektur yang telah banyak digunakan pada penelitian dan publikasi terkait IoT. Ketiga model tersebut mengadopsi model arsitektur berbasis *layer* yang membagi sistem dan aplikasi IoT menjadi beberapa *layer*. Ketiga model arsitektur IoT tersebut dijelaskan secara singkat sebagai berikut.

A. Model Tiga Layer

Gbr. 1 menunjukkan model arsitektur IoT tiga *layer* yang merupakan model referensi pertama yang diusulkan untuk sistem IoT [9]. Model ini dapat dipandang sebagai bentuk pengembangan dari model arsitektur *Wireless Sensor Networks* (WSN) yang dikombinasikan dengan server awan (*cloud server*), yang pada akhirnya menyediakan layanan terhadap aplikasi dan pengguna sistem IoT.

B. Model Lima Layer

Model arsitektur lima *layer* merupakan alternatif model sistem IoT yang diusulkan untuk memfasilitasi interaksi antara



Gbr. 2 Model arsitektur IoT lima *layer*.

bagian-bagian dalam sebuah *enterprise* dengan membagi sistem yang kompleks menjadi aplikasi-aplikasi yang lebih sederhana dengan komponen-komponen yang didefinisikan dengan baik [10]. Model arsitektur ini ditunjukkan pada Gbr. 2.

C. Model Tujuh Layer

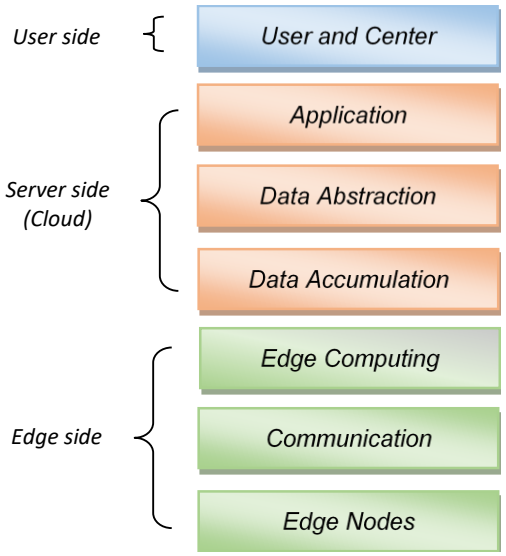
Pada tahun 2014, Cisco mengusulkan model arsitektur IoT yang terdiri atas tujuh *layer* [11], seperti yang ditunjukkan pada Gbr. 3. Adapun deskripsi dari tiap-tiap *layer* pada model arsitektur tersebut adalah sebagai berikut.

1) Layer 1-Edge Nodes: Layer paling bawah ini biasanya tersusun atas peranti-peranti seperti sensor, pengendali-pintar, pembaca RFID, aktuator, dan semacamnya. Kerahasiaan dan integritas data harus dipertimbangkan mulai dari *layer* ini dan juga diteruskan pada *layer* di atasnya.

2) Layer 2-Communication: Layer ini terdiri atas semua komponen terkait pengiriman data (informasi) dan juga perintah (*command*). Media komunikasi ini bertanggung jawab untuk menyediakan sarana komunikasi antar peranti pada *layer node*, antar komponen pada *layer* kedua, dan transmisi data antara *layer* kedua dan ketiga (*edge computing layer*).

3) Layer 3-Edge Computing: Level ketiga ini sering juga dikenal dengan istilah *fog computing.* Pada level ini pemrosesan data sederhana diinisiasi. Langkah ini dimaksudkan untuk mengurangi beban komputasi pada level yang lebih tinggi dan juga untuk mempercepat respons. Sebagian besar aplikasi *realtime* perlu melakukan komputasi sedekat mungkin dengan peranti IoT. Besar kecilnya pemrosesan pada level ini tergantung pada kekuatan komputasi penyedia layanan, server, dan *node* komputasi. Pada *layer* ini, biasanya digunakan metode pemrosesan sinyal dan algoritme pembelajaran sederhana.

4) Layer 4-Data Accumulation: Banyak aplikasi IoT yang tidak memerlukan pengolahan data secara langsung. *Layer* ini memungkinkan pengubahan format data untuk keperluan analisis data ataupun berbagi dengan server komputasi pada level yang lebih tinggi. Tugas utama *layer* ini adalah mengubah format keluaran sensor IoT menjadi format yang cocok untuk penyimpanan di basis data, termasuk juga memfilter dan mengurangi data serta menentukan sebuah data perlu diteruskan untuk proses pada level yang lebih tinggi atau tidak.



Gbr. 3 Model arsitektur IoT tujuh *layer*.

5) Layer 5-Data Abstraction: Layer ini memfasilitasi pengolahan dan penyimpanan data sehingga proses pengolahan tahap selanjutnya menjadi lebih sederhana dan efisien. Pengolahan data termasuk proses normalisasi atau denormalisasi, penentuan indeks, konsolidasi data, dan penyediaan akses pada *multiple data store*.

6) Layer 6-Application: Layer aplikasi menyediakan proses interpretasi informasi. Aplikasi IoT pada level ini akan banyak membutuhkan koordinasi dengan *layer* abstraksi data dan akumulasi data. Aplikasi IoT sangat beragam, bergantung pada domain aplikasi dan proses bisnis organisasi.

7) Layer 7-User dan Center: Pada *layer* ini, pengguna akan memanfaatkan aplikasi dan juga informasi hasil proses olah data yang dilakukan pada *layer-layer* di bawahnya. Penerapan IoT pada *layer* ini dapat juga merupakan pusat data bagi suatu *enterprise*.

IV. Ancaman Keamanan pada *Internet of Things*

Salah satu tantangan yang harus diatasi untuk mendorong implementasi IoT secara luas adalah faktor keamanan. IoT merupakan sebuah sistem kompleks yang melibatkan banyak komponen. Kompleksitasnya bukan hanya karena keterlibatan berbagai entitas seperti data, perangkat, jalur komunikasi, sensor, dan lain-lain, tetapi juga karena melibatkan berbagai peralatan dengan beragam kemampuan komunikasi dan pengolahan data. Banyaknya entitas dan data yang terlibat membuat IoT menghadapi risiko keamanan yang dapat mengancam dan membahayakan konsumen. Ancaman ini dapat berupa akses oleh orang yang tidak berhak untuk mengakses data dan menyalahgunakan informasi personal, memfasilitasi serangan terhadap sistem yang lain, serta mengancam keselamatan personal penggunanya. Ancaman-ancaman yang dapat memengaruhi entitas IoT sangat beragam, tergantung pada target serangan tersebut.

Sistem keamanan konvensional tidak dapat langsung diterapkan pada sistem IoT [12]. Hal ini disebabkan objek-

TABEL I
KEBUTUHAN KEAMANAN IOT

Parameter	Definisi	Kode
Confidentiality	Menjamin hanya pengguna sah yang dapat mengakses informasi.	C
Integrity	Menjamin akurasi, konsistensi data, serta mencegah manipulasi data	I
Availability	Menjamin ketersediaan layanan, data, dan informasi bagi pengguna yang sah	A
Accountability	Kemampuan sistem mencatat aktivitas sistem dan pengguna	AC
Auditability	Kemampuan untuk melakukan pemantauan seluruh proses dalam sistem	AU
Trustworthiness	Kemampuan memverifikasi identitas dan menentukan *trust* dengan pihak ketiga	TW
Non-repudiation	Kemampuan sistem melakukan konfirmasi ada atau tidaknya sebuah aksi	NR
Privacy	Menjamin agar sistem patuh terhadap kebijakan privasi dan memungkinkan pengguna mengontrol data pribadinya.	P

objek dalam IoT bersifat dinamis, dalam arti objek-objek (peranti) dapat dengan bebas bergabung ataupun memisahkan diri dari komunitas IoT tempat objek-objek tersebut bergabung. Karakteristik lain yang sangat berpengaruh adalah keterbatasan sumber daya dari objek-objek IoT, baik terkait sumber daya (*power*), kecepatan pemrosesan (CPU), memori, kapasitas kanal (*bandwidth*), dan sebagainya [13]. Karakteristik-karakteristik inilah yang menjadikan karakteristik model keamanan pada IoT berbeda dibandingkan sistem keamanan jaringan konvensional.

Aspek keamanan pada sistem teknologi informasi secara umum dapat diklasifikasikan menjadi tiga kategori yang dikenal dengan istilah *CIA-Triad*, yakni: (i) *confidentiality*, (ii) *integrity*, dan (iii) *availability*. Konsep *CIA-Triad* belum cukup untuk mendefinisikan aspek keamanan pada sistem yang melibatkan kolaborasi antara banyak pihak seperti halnya pada IoT. Telah dibuat daftar yang lebih komprehensif tentang karakteristik keamanan dengan menganalisis berbagai sumber informasi dan literatur terkait keamanan [14]. Tabel I menampilkan daftar kebutuhan parameter keamanan pada IoT serta penjelasan dan definisinya.

A. Ancaman Keamanan IoT pada Layer Nodes

Sistem dan aplikasi IoT mulai banyak diimplementasikan pada berbagai macam aplikasi dari manajemen industri sampai pemantau kesehatan pribadi. Hal ini membuat sistem dan aplikasi IoT menarik bagi para penyerang untuk dijadikan target serangan, apapun motivasinya.

Salah satu motivasi penyerang sistem IoT adalah pencurian data dan informasi sensitif, seperti nomor kartu kredit, informasi lokasi, *password* akun bank, dan data terkait kesehatan, dengan cara mengeksploitasi kelemahan-kelemahan pada sistem IoT.

1) Edge Node: Peranti IoT yang sering dijumpai pada *edge node* antara lain *RFID readers*, sensor, dan *node* aktuator. Serangan yang utama pada *edge node* ini adalah sebagai berikut [15].

- *Hardware Trojan.* Serangan jenis *hardware Trojan* menyerang dengan melakukan modifikasi pada *Integrated Circuit* (IC) yang memungkinkan penyerang mendapatkan akses terhadap data atau perangkat lunak yang dijalankan pada IC tersebut [16]. Untuk dapat memasukkan *Trojan*, penyerang melakukan pengubahan pada desain IC sebelum atau pada saat fabrikasi dan menentukan mekanisme *trigger* yang akan mengaktifkan *Trojan* tersebut. Mekanisme pengaktifan *Trojan* ini dapat dilakukan dengan dua cara: i) internal, yang akan aktif ketika suatu kondisi yang telah didefinisikan terpenuhi; dan ii) eksternal, yang akan mengaktifkan *Trojan* dengan perantara suatu antena atau sensor yang dapat berinteraksi dengan dunia luar.
- *Non-network side-channel attack.* Setiap *node* dapat membuka informasi sensitif pada kondisi operasi normal, bahkan ketika peranti tidak menggunakan media komunikasi nirkabel untuk transmisi data, misalnya *beacon* yang selalu memancarkan status peranti. Kerentanan seperti ini dapat menjadi isu terkait privasi pada sistem medis. Contohnya adalah seorang pasien yang mengenakan peranti medis yang mengindikasikan kondisi medis tertentu yang berdampak pada stigma sosial. Hal semacam ini dapat membuat malu pasien jika penyakit yang diderita dipersepsikan negatif. Selain itu, peranti IoT medis dapat juga membuka informasi kesehatan personal, seperti tekanan darah, kadar gula, dan sebagainya.
- *Battery draining*. Karena keterbatasan ukuran, biasanya peranti IoT hanya memiliki baterai dengan kapasitas kecil. Oleh karena itu, serangan ini dapat berdampak serius karena peranti akan mengalami kegagalan operasi dan gagal mengakuisisi data terutama di saat-saat darurat. Misalnya, penyerang dapat menemukan cara untuk menguras baterai detektor asap, maka penyerang dapat menggagalkan alarm sistem pendeteksi kebakaran pada gedung tersebut. Pada contoh lain, si penyerang dapat mengirimkan ribuan atau jutaan paket acak yang meminta respons dari peranti IoT sehingga peranti tersebut dapat menguras sumber daya (baterai) peranti tersebut.
- *Sleep deprivation.* Serangan bertipe DOS ini menargetkan peranti dengan kapasitas energi terbatas. Pada serangan ini, penyerang mengirimkan sejumlah permintaan yang terlihat asli. Oleh karena itu, jenis serangan ini lebih sulit dideteksi. Salah satu serangan jenis ini adalah serangan *sleep deprivation* pada peranti dengan sumber daya baterai terbatas [17].
- *Outage attack*. Serangan ini terjadi ketika sebuah peranti IoT (*edge node*) gagal beroperasi normal. Dalam beberapa kasus, sejumlah peranti atau peranti koordinator berhenti berfungsi. Kegagalan ini dapat disebabkan oleh kesalahan

pada proses manufaktur, terkurasnya baterai, *sleep deprivation*, injeksi kode, atau akses ilegal secara fisik ke peranti. Salah satu contoh yang terkenal adalah serangan injeksi kode Stuxnet pada program pengendali proses nuklir Iran [18].

- *Physical attack (tampering)*. Peranti IoT sering kali berada pada lingkungan fisik yang rawan (perkebunan, perikanan, jalan, peternakan, dan sebagainya) sehingga membuatnya rentan terhadap serangan-serangan fisik. Dengan akses secara langsung, penyerang dapat mengekstrak informasi kriptografi, memodifikasi rangkaian, mengubah kode program, atau mengubah sistem operasi. Bahkan, lebih jauh lagi, penyerang dapat merusak peranti secara permanen. Salah satu contoh adalah serangan pada Nest Thermostat, yaitu penyerang berusaha mengubah *default firmware* dengan yang palsu. Dengan cara ini, penyerang dapat mengontrol termostat bahkan ketika penyerang sudah tidak dapat mengakses secara langsung.
- *Node replication attack*. Pada serangan ini, penyerang memasang sebuah *node* baru pada sekumpulan *node* yang telah ada dengan cara mereplikasi salah satu identitas *node* lain.
- *Camouflage attack*. Pada serangan tipe ini, penyerang menambahkan *node* palsu atau menyerang (memodifikasi) *node* yang sah untuk menyembunyikan keberadaan serangan tersebut. Setelah itu *node* yang telah dimodifikasi dapat beroperasi secara normal seperti biasa.

2) Tag RFID: Salah satu peranti *edge-node* yang banyak digunakan pada sistem IoT adalah *tag* RFID. Ada beberapa jenis serangan pada *tag* RFID, antara lain sebagai berikut.

- *Tracking*. Peranti RFID memiliki identitas unik. Akibatnya, penyerang dapat menggunakan peranti *RFID-reader* yang tidak sah untuk membaca identitas *tag* RFID tersebut. Peluang pembacaan tersebut dapat dimanfaatkan penyerang untuk melakukan pelacakan terhadap suatu objek yang menjadi target serangan.
- *Inventorying.* Ada tipe *tag* tertentu yang memuat informasi berharga tentang produk tempat RFID tersebut terpasang. Misalnya, *tag Electronic Product Code* (EPC) memiliki dua komponen: kode manufaktur dan kode produk. Akibatnya, seorang individu yang memiliki *tag* EPC biasanya menggunakan standar inventarisasi [19], sehingga pembaca *tag* dapat memeriksa produk yang dimiliki individu tersebut. Ancaman ini mengarah pada masalah privasi. Misalnya, penyerang mungkin mengenali jenis alat kesehatan tertentu, misalnya pompa insulin yang dikenakan pasien, sehingga penyerang dapat mengetahui bahwa individu tersebut menderita diabetes.
- *Tag cloning.* Serangan *tag cloning* (*spoofing*) dapat sangat menguntungkan peretas dan sangat berbahaya bagi reputasi perusahaan. Kerusakan dapat diperparah melalui otomatisasi serangan [20]. Penyerang dapat menggunakan kloning *tag* untuk mengakses area terlarang di perusahaan, informasi rekening bank, atau informasi sensitif lainnya.
- *DoS Attack.* Dalam serangan DoS yang menyerang *tag* RFID, kanal frekuensi radio diganggu sehingga *tag* tidak dapat dibaca oleh pembaca *tag* dan akibatnya layanan menjadi tidak tersedia. Sebagai contoh, seorang penyerang dapat mengunci seluruh bangunan dengan mengacaukan semua pintu berbasis RFID. Kerentanan tambahan protokol autentikasi RFID terhadap serangan DOS telah didiskusikan pada penelitian sebelumnya [21].

B. Ancaman Keamanan pada Layer Komunikasi

Serangan yang terjadi pada *layer* komunikasi dapat berupa hal-hal sebagai berikut.

1) Eavesdropping: Serangan ini mengacu kepada aksi penyerang dengan cara mencuri dengar dengan sengaja pertukaran data yang terjadi pada kanal komunikasi. Jika data tidak dienkripsi, penyerang dapat membaca dan mengumpulkan data penting seperti *username* dan *password*, serta data lain seperti informasi *access control*, konfigurasi *node*, *share network password*, dan identitas *node*. Penyerang dapat mengolah dan memanfaatkan data yang tertangkap untuk menyusun serangan terencana. Misalnya, jika si penyerang dapat mengekstrak informasi yang diperlukan untuk menambahkan sebuah *node* yang sah, penyerang akan dengan mudah menambahkan *node* palsu di dalam sistem.

2) Side Channel Attack: Serangan jenis ini merupakan serangan yang kuat terhadap enkripsi, walaupun relatif sulit untuk diimplementasikan. Serangan jenis ini biasanya termasuk noninvasif. Penyerang biasanya hanya mengekstrak informasi yang tanpa sengaja bocor. Misalnya, informasi tentang jarak antar paket yang berurutan, pita frekuensi, dan modulasi yang digunakan. Salah satu ciri serangan ini adalah tidak mudah terdeteksi sehingga akan lebih sulit untuk menghindarinya. Salah satu hal yang dapat dilakukan adalah meminimalkan kebocoran informasi atau menambahkan derau pada informasi yang rentan bocor.

3) Serangan Denial of Service (DoS): Serangan DoS yang paling umum pada kanal komunikasi adalah *jamming* terhadap sinyal radio. Ada dua jenis serangan ini. Serangan yang pertama adalah *continuous jamming*, yang dilakukan secara terus menerus. Serangan ini bertujuan untuk melumpuhkan jaringan komunikasi. Serangan jenis kedua yaitu *intermittent jamming*, yang dilakukan secara periodik. Serangan ini bertujuan untuk melemahkan kinerja sistem yang peka terhadap waktu (*time sensitive*).

4) Injecting Fraudulent Packet: Seorang penyerang dapat menginjeksikan paket palsu ke dalam kanal komunikasi menggunakan tiga metode serangan yang berbeda: (i) penyisipan, (ii) manipulasi, dan (iii) replikasi (juga disebut *replay attack*) [22]. Dalam skenario penyisipan, penyerang memasukkan paket baru dalam komunikasi jaringan. Dengan kata lain, serangan penyisipan memiliki kemampuan untuk menghasilkan dan mengirim paket jahat yang tampaknya sah. Serangan manipulasi melibatkan penangkapan paket dan kemudian memodifikasinya, misalnya dengan mengubah *header*, *checksum*, dan data, kemudian mengirim paket yang dimanipulasi. Dalam serangan replikasi, penyerang menangkap paket yang sebelumnya telah dipertukarkan antara dua entitas untuk memutar ulang (*replay*) paket yang sama.

5) Routing Attack: Serangan yang memengaruhi cara pesan diteruskan disebut serangan *routing*. Seorang penyerang dapat menggunakan serangan seperti ini untuk menipu, mengarahkan, menyesatkan, atau menghapus paket pada *layer* komunikasi. Jenis serangan perutean yang paling sederhana adalah serangan perubahan, yaitu penyerang mengubah informasi perutean, misalnya dengan membuat *routing loop* atau pesan kesalahan palsu [16].

C. Ancaman Keamanan pada Edge Computing

Edge computing (*fog computing*) merupakan arsitektur yang muncul seiring perkembangan topologi dan infrastruktur pada sistem IoT. Pada arsitektur IoT tujuh *layer* (Gbr. 3), *edge-computing* ini merupakan komponen pada *layer* 3. Demikian juga ancaman dan kerentanan keamanannya belum banyak dieksplorasi. Berikut ini beberapa skenario serangan yang sering terjadi pada *edge computing*.

1) Malicious Injection: Validasi masukan (*input*) yang tidak memadai memungkinkan datangnya serangan berupa injeksi masukan berbahaya. Penyerang dapat menyuntikkan masukan jahat yang menyebabkan penyedia layanan menjalankan suatu perintah (aktivitas) atas nama penyerang. Misalnya, penyerang dapat menambahkan komponen yang tidak sah ke salah satu level di bawah *computing node* ini (level komunikasi atau *edge node*) yang mampu menyuntikkan masukan berbahaya ke server. Setelah itu, penyerang dapat mencuri data, mengganggu integritas basis data, atau memotong autentikasi. Pesan kesalahan basis data standar yang ditampilkan oleh server basis data juga dapat dimanfaatkan penyerang. Dalam situasi ketika penyerang tidak memiliki pengetahuan tentang tabel basis data, penyerang dapat dengan sengaja membuat skrip yang dapat membangkitkan *exception* untuk mengungkapkan rincian lebih lanjut tentang setiap tabel dan nama-nama kolomnya [23].

2) Integrity Attack Against Machine Learning: Dua jenis serangan dapat diluncurkan terhadap metode *machine learning* yang digunakan dalam sistem IoT, yaitu kausatif dan eksplorasi. Dalam serangan kausatif, penyerang mengubah proses pelatihan dengan memanipulasi *dataset* pelatihan, sedangkan dalam serangan eksplorasi, penyerang mengeksploitasi kerentanan tanpa mengubah proses pelatihan. Penelitian baru-baru ini telah memperkenalkan jenis baru serangan kausatif, yang disebut *poisoning attack* [24], [25]. Dalam *poisoning attack*, penyerang menambahkan data invalid yang dipilih secara khusus ke dalam *dataset* pelatihan. Dalam sistem berbasis *edge-computing*, penyerang dapat meluncurkan serangan ini terhadap algoritme pembelajaran dengan secara langsung mengakses server atau *node* komputasi, atau mungkin dapat menambahkan data berbahaya ke *dataset* dengan menambahkan cukup banyak *node* palsu ke dalam sistem IoT. Motivasi utamanya adalah untuk menyebabkan algoritme klasifikasi menyimpang dari pembelajaran model yang valid dengan memanipulasi *dataset*.

Gbr. 4 merangkum jenis-jenis serangan yang sering menyerang sistem IoT, baik pada *layer* sensor, *layer* komunikasi, maupun *layer* komputasi pada server. Target serangan (C, I, A, AC, AU, TW, NR, P) mengacu pada terminologi pada Tabel I. Berkembangnya jenis serangan pada teknologi IoT ini telah membawa dampak pada munculnya ancaman keamanan dan serangan terhadap privasi dan keamanan peranti-peranti sehingga diperlukan studi lebih lanjut tentang cara-cara penanganan dan pencegahan serangan pada sistem IoT.

V. Solusi Keamanan pada *Internet of Things*

Pada bagian ini didiskusikan solusi-solusi keamanan yang perlu diimplementasikan pada tiap *layer* untuk menanggulangi ancaman-ancaman keamanan sebagaimana telah didiskusikan pada bagian sebelumnya.

A. Solusi Keamanan pada Edge Node

Pada subbagian ini didiskusikan solusi keamanan yang dapat dilakukan untuk mengatasi ancaman-ancaman keamanan sistem IoT pada sisi *edge-node* (*layer* 1 pada Gbr. 3). Berikut adalah beberapa solusi keamanan yang dapat dilakukan untuk mengatasi ancaman-ancaman keamanan sistem IoT pada sisi *edge-node*.

1) Side-Channel Analysis: Metode ini menyediakan pendekatan yang efektif untuk mendeteksi *hardware-trojan* dan *firmware* berbahaya yang dipasang pada perangkat IoT. Adanya *Trojan* pada *firmware* peranti IoT akan menyebabkan dampak negatif pada penggunaan baterai, adanya efek tunda waktu, dan perubahan distribusi panas pada IC. Untuk mendeteksi *hardware-trojan*, mekanisme deteksi *Trojan* berbasis sinyal dapat dilakukan dengan membandingkan karakteristik fisik dan/atau peta distribusi panas dari IC yang mencurigakan dengan karakteristik dari IC lain yang bebas *Trojan* [26].

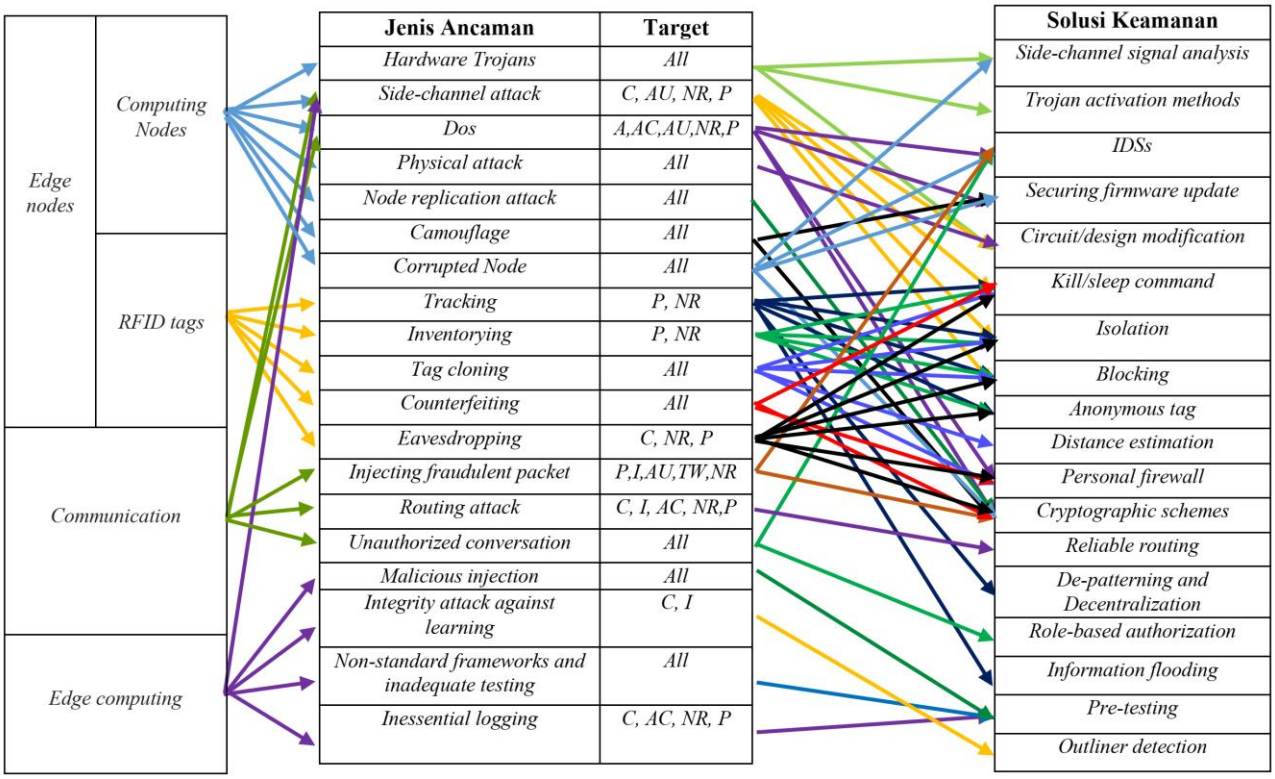
2) Malicious Firmware Detection: Efektivitas analisis sinyal dalam mendeteksi *firmware* yang diinstal pada perangkat telah ditunjukkan oleh beberapa upaya penelitian sebelumnya [27]. Analisis sinyal ini dapat mengungkapkan informasi berharga tentang operasi perangkat. Mirip dengan mekanisme deteksi *Trojan*, metode deteksi *malware* dapat memproses sinyal untuk mendeteksi perilaku abnormal perangkat, misalnya peningkatan konsumsi daya yang signifikan, yang merupakan hasil dari *malware* yang aktif pada perangkat.

3) Policy-based Mechanism and Intrusion Detection System: Metode berbasis kebijakan (*policy*) merupakan salah satu teknik yang menjanjikan untuk menyelesaikan permasalahan keamanan dan privasi pada level *node* ini. Pelanggaran kebijakan penting dapat dideteksi secara berkelanjutan dengan memperkenalkan *Intrusion Detection System* (IDS) [28].

B. Solusi Keamanan pada RFID Node

Berikut adalah beberapa solusi keamanan yang dapat dilakukan untuk mengatasi ancaman-ancaman keamanan sistem IoT pada sisi *edge-node* untuk jenis peranti RFID.

1) Kill-Sleep Command: Skenario ini dimasukkan ke dalam proses pembuatan *tag* RFID. *Tag* RFID memiliki PIN unik, misalnya 32-bit. Setelah menerima PIN yang benar dari



Gbr. 4 Kategori, jenis, dan target serangan serta solusi keamanan pada sistem IoT.

pembaca RFID, *tag* dapat dinonaktifkan sehingga *tag* tidak akan dapat mengirimkan informasi lebih lanjut setelah menerima perintah ini [29]. Ada pendekatan alternatif yang disebut perintah *sleep* yang membuat *tag* tertidur, misalnya dengan membuatnya tidak aktif untuk periode waktu tertentu [19]. Meskipun ide-ide ini tampak sederhana, perancangan dan implementasi manajemen PIN yang aman dan efektif membutuhkan teknik-teknik canggih.

2) Isolation: Cara yang sangat efektif untuk melindungi privasi *tag* adalah dengan mengisolasinya dari semua gelombang elektromagnet. Salah satu caranya adalah dengan membuat dan menggunakan ruang isolasi. Namun, membangun kamar seperti itu biasanya sangat mahal. Pendekatan alternatifnya adalah dengan menggunakan wadah isolasi yang biasanya terbuat dari jaring logam [19]. Wadah ini, yang dapat memblokir gelombang elektromagnetik dari frekuensi tertentu, disebut sangkar Faraday [30]. Pendekatan lain adalah menghentikan semua saluran radio terdekat menggunakan *RF jammer* aktif yang terus-menerus mengganggu saluran RF tertentu.

C. Solusi Keamanan pada Kanal Komunikasi

Pada subbagian ini didiskusikan solusi keamanan untuk mengatasi ancaman-ancaman keamanan sistem IoT pada kanal komunikasi (*layer* ke-2 pada Gbr. 3).

1) Reliable Routing: Karakteristik penting dari jaringan IoT yang mempersulit implementasi protokol *routing* adalah bahwa *node* atau server perantara memerlukan akses langsung ke isi pesan sebelum meneruskannya. Seperti disebutkan sebelumnya, beberapa serangan valid terhadap *routing* telah diusulkan dalam literatur. Suatu penelitian telah membahas sebagian besar skenario serangan utama yang terjadi pada proses *routing* [31]. Penelitian ini telah memberikan analisis keamanan terperinci dari protokol *routing* utama dan serangan terhadapnya, bersama dengan tindakan pengamanannya. Berbagai upaya penelitian lain juga telah mencoba mengatasi masalah keamanan dan privasi dalam *routing* [32].

2) Intrusion Detection System (IDS): Metode IDS ini sangat penting dilakukan pada *layer* komunikasi untuk memonitor operasional jaringan dan jalur komunikasi dan juga untuk mendeteksi terjadinya anomali pada jaringan, misalnya ketika sebuah *policy* yang telah didefinisikan sebelumnya dilanggar oleh pengguna. SVELTE [33] adalah salah satu IDS pertama yang dirancang untuk memenuhi persyaratan *node* IoT yang terhubung dengan IPv6. IDS ini mampu mendeteksi serangan *routing*, seperti informasi palsu atau telah diubah dan serangan *black hole*.

3) Kriptografi: Penggunaan skema kriptografi untuk mengamankan protokol komunikasi adalah salah satu pertahanan paling efektif terhadap berbagai serangan, termasuk penyadapan dan serangan *routing* yang sederhana, pada *layer* komunikasi. Beberapa metode enkripsi telah diusulkan untuk mengatasi masalah keamanan dalam komunikasi [34], [35]. Teknik enkripsi-dekripsi, yang dikembangkan untuk jaringan kabel tradisional, tidak secara langsung berlaku untuk sebagian besar komponen IoT, khususnya untuk *edge-node* yang bertenaga baterai kecil. *Edge-node* biasanya berupa sensor

kecil yang memiliki kapasitas baterai, daya pemrosesan, dan memori yang terbatas. Penggunaan enkripsi meningkatkan penggunaan memori, konsumsi energi, penundaan, dan kehilangan paket [36]. Varian AES telah menghasilkan hasil yang menjanjikan untuk menyediakan komunikasi yang aman pada IoT. Selain itu, berbagai metode enkripsi ringan telah diusulkan, misalnya CLEFIA [37] dan PRESENT [38]. Sayangnya, saat ini belum ada metode enkripsi kunci publik yang menyediakan keamanan yang cukup sekaligus memenuhi persyaratan yang ringan [36].

4) De-patterning and Decentralization: De-patterning dan *decentralization* merupakan dua metode utama yang diusulkan untuk memberikan anonimitas dan pertahanan terhadap *side-channel attack*. Selalu ada *trade-off* antara anonimitas dan kebutuhan untuk berbagi informasi. Pengacakan pola transmisi data dapat melindungi sistem dari serangan *side-channel*, misalnya dengan menyisipkan paket tambahan yang dapat mengubah pola trafik sehingga pola yang terbentuk tidak dapat dikenali. Metode alternatif untuk memastikan anonimitas adalah distribusi data sensitif melalui *spanning tree* sehingga tidak ada *node* yang memiliki tampilan lengkap dari data asli. Metode ini disebut desentralisasi [39].

5) Rule-based Authorization: Salah satu solusi keamanan dapat diimplementasikan dengan menerapkan metode *rule-based authorization*. Untuk mencegah respons yang tidak perlu, seperti terhadap permintaan oleh *node* pengganggu atau penyusup, sistem otorisasi berbasis peran (*role-based authorization*) memverifikasi komponen, seperti *edge-node*, penyedia layanan, atau *router*, dapat mengakses, berbagi, atau mengubah informasi atau tidak. Selain itu, untuk setiap komunikasi, sistem otorisasi harus memeriksa kedua pihak yang terlibat dalam interaksi tersebut telah divalidasi dan memiliki wewenang yang diperlukan atau belum [40].

D. Solusi Keamanan pada Computing Layer

Pada subbagian ini didiskusikan solusi keamanan untuk mengatasi ancaman-ancaman keamanan sistem IoT pada *computing level* (*layer* 3 pada Gbr. 3).

1) Pre-Testing: Pengujian terhadap proses pembaruan dan implementasi desain penting untuk dilakukan sebelum desain tersebut digunakan dalam sistem IoT. Perilaku seluruh sistem dan komponennya, seperti *router*, *edge-node*, dan server, harus diperiksa dengan teliti dengan memasukkan masukan yang berbeda ke sistem dan memantau keluaran. Secara khusus, upaya prapengujian dilakukan untuk mengidentifikasi kemungkinan skenario serangan dan menyimulasikan skenario ini untuk melihat cara sistem merespons [41]. Ini juga menentukan informasi yang harus dicatat dan informasi yang terlalu sensitif untuk disimpan. Selain itu, *file* masukan harus diperiksa dengan cermat untuk mencegah bahaya injeksi. Sebagai contoh, penyerang seharusnya tidak dapat menjalankan perintah apa pun dengan menyuntikkannya ke *file* masukan.

2) Outlier Detection: Tujuan pertahanan keamanan terhadap serangan integritas data pada metode *machine learning* adalah untuk mengurangi pengaruh penambahan data invalid terhadap hasil. Data invalid ini merupakan *outlier* (penyimpangan) pada *dataset* yang digunakan. Sebuah *framework* untuk pertahanan terhadap serangan jenis *poisoning* telah dikembangkan berdasarkan statistik untuk mengurangi efek keracunan [42]. Penelitian lain telah melaporkan beberapa teknik penanggulangan serangan *poisoning* di bidang perawatan kesehatan [43].

VI. Tantangan Baru Riset Keamanan IoT

Pada pembahasan sebelumnya, beberapa serangan terhadap keamanan IoT telah diuraikan disertai dengan teknik-teknik penanganannya. Pada bagian ini didiskusikan dua kategori tantangan keamanan IoT yang belum dibahas pada literatur sebelumnya.

A. Pertumbuhan Secara Eksponensial Kanal Komunikasi yang Rentan

Sebagian besar layanan berbasis IoT mengandalkan perangkat bertenaga baterai dengan penyimpanan terbatas dan sumber daya komputasi. Karena karakteristik khusus dari perangkat ini dan faktor biaya yang dianggap penting oleh produsen, beberapa perangkat yang sudah ada di pasaran tidak mendukung protokol kriptografi yang aman. Ini telah menyebabkan munculnya sejumlah besar jalur komunikasi dalam jaringan yang dapat dimanfaatkan oleh penyerang untuk menargetkan serangan pada entitas yang diasumsikan sudah aman. Beberapa upaya penelitian menunjukkan kemungkinan penyerangan terhadap *edge node* untuk mengekstrak kata sandi Wi-Fi dari sebuah rumah cerdas [44], [45]. Telah ditunjukkan sebuah bola lampu yang terhubung ke internet dapat mengungkapkan kata sandi Wi-Fi pengguna kepada penyerang [45]. Berkembangnya aplikasi IoT yang semakin luas pada hampir semua domain aplikasi akan semakin memperbesar dampak jenis serangan pada *edge-node* ini.

B. Penyalahgunaan Data

Dengan semakin banyaknya aplikasi dan implementasi IoT pada masyarakat modern ini, semakin banyak pula sensor-sensor yang terpasang dan terkoneksi dengan internet. Beberapa penelitian telah melaporkan adanya penggunaan data yang tidak semestinya atas beberapa jenis data terkait pengguna ataupun lingkungan aplikasi IoT [46], [47]. Salah satu penelitian mendeskripsikan sejumlah daftar informasi sensitif terkait privasi, seperti jumlah penghuni, kebiasaan personal, dan rutinitas harian, yang dapat disimpulkan dari analisis data penggunaan listrik yang dikumpulkan pada aplikasi rumah-cerdas [48].

Platform telekomunikasi seluler modern seperti peranti pintar (Android, iPhone, dan semacamnya) memungkinkan aplikasi membaca penggunaan daya pada ponsel pintar. Informasi ini dianggap tidak berbahaya dan membacanya tidak memerlukan izin atau pemberitahuan pengguna. Sebuah penelitian menunjukkan bahwa dengan hanya membaca konsumsi daya telepon selama beberapa menit, sebuah aplikasi dapat mempelajari informasi tentang lokasi pengguna [49]. Dengan menggunakan algoritme *machine learning*, penyerang

dapat mengolah data yang telah dikumpulkan dan melakukan estimasi terhadap lokasi telepon pengguna tersebut.

VII. KESIMPULAN

Berkembangnya teknologi IoT pada dasawarsa terakhir ini telah membawa dampak pada munculnya ancaman keamanan dan serangan terhadap privasi dan keamanan peranti-peranti IoT. Sayangnya, ancaman-ancaman keamanan tersebut belum teridentifikasi dengan jelas pada domain IoT. Paparan dalam makalah ini telah merangkum jenis serangan, ancaman, serta kemungkinan cara pertahanan (solusi) terhadap ancaman keamanan tersebut. Tinjauan keamanan ini dapat memberikan gambaran tipikal serangan pada sistem IoT, tipe serangan yang sudah dapat ditangani, serta jenis serangan yang masih memerlukan penelitian lanjut. Dengan semakin berkembangnya adopsi teknologi IoT pada banyak bidang, ancaman keamanan pada IoT ini memerlukan perhatian dan solusi dari komunitas akademisi, peneliti, maupun pihak industri.

REFERENSI

[1] M.A. Iqbal, O.G. Olaleye, dan M.A. Bayoumi, "A Review on Internet of Things (IoT): Security and Privacy Requirements and the Solution Approaches," *Glob. J. Comput. Sci. Technol. E Network, Web Secur.*, Vol. 16, No. 7, hal. 1-10, 2016.

[2] Project CASAGRAS, "CASAGRAS Final Report: RFID and the Inclusive Model for the Internet of Things," *Sci. Am.*, Vol. 291, No. 4, hal. 10–12, 2009.

[3] R. Minerva, A. Biru, dan D. Rotondi, "Toward a Definition of the Internet of Things," *IEEE Internet of Things*, hal. 1–86, 2015.

[4] M.M. Kermani, M. Zhang, A. Raghunathan, dan N.K. Jha, "Emerging Frontiers in Embedded Security," *Proc. IEEE Int. Conf. VLSI Des.*, 2013, hal. 203–208.

[5] A.M. Nia, M. Mozaffari-kermani, S. Sur-Kolay, A. Raghunathan, dan N.K. Jha, "Energy-Efficient Long-term Continuous Personal Health Monitoring," *IEEE Trans. Multi-Scale Comput. Syst.*, Vol. 1, No. 2, hal. 85–98, 2015.

[6] P. Alinia, R. Saeedi, R. Fallahzadeh, A. Rokni, dan H. Ghasemzadeh, "A Reliable and Reconfigurable Signal Processing Framework for Estimation Metabolic Equivalent of Task in Wearable Sensors," *IEEE J. Sel. Top. Signal Process.*, Vol. 10, No. 5, hal. 842 - 853, 2016.

[7] K. Su, J. Li, dan H. Fu, "Smart City and the Applications," *2011 Int. Conf. Electron. Commun. Control. ICECC 2011 - Proc.*, 2011, hal. 1028–1031.

[8] M.T. Lazarescu, "Design of a WSN Platform for Long-Term Environmental Monitoring for IoT Applications," *IEEE J. Emerg. Sel. Top. Circuits Syst.*, Vol. 3, No. 1, hal. 45–54, Mar. 2013.

[9] S. Vashi, J. Ram, J. Modi, S. Verma, dan C. Prakash, "Internet of Things (IoT): A Vision, Architectural Elements, and Security Issues," *2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*, 2017, hal. 492–496.

[10] L. Atzori, A. Iera, dan G. Morabito, "The Internet of Things: A Survey," *Comput. Networks*, Vol. 54, No. 15, hal. 2787–2805, Okt. 2010.

[11] Cisco, "The Internet of Things Reference Model," *Cisco White Paper*, San Jose, CA: Cisco Systems, 2014.

[12] R. Roman, P. Najera, dan J. Lopez, "Securing the Internet of Things," *Computer (Long. Beach. Calif).*, Vol. 44, No. 9, hal. 51–58, Sep. 2011.

[13] C. Maple, "Security and Privacy in the Internet of Things," *J. Cyber Policy*, Vol. 2, No. 2, hal. 155–184, 2017.

[14] Y. Cherdantseva dan J. Hilton, "A Reference Model of Information Assurance & Security," *Proc. - 2013 Int. Conf. Availability, Reliab. Secur. ARES 2013*, 2013, hal. 546–555.

[15] H. Salmani, M.M. Tehranipoor, dan S. Member, "Vulnerability Analysis of a Circuit Layout to Hardware Trojan Insertion," *IEEE Trans. Inf. Forensics Secur.*, Vol. 11, No. 6, hal. 1214–1225, 2016.

[16] A. Mosenia dan N.K. Jha, "A Comprehensive Study of Security of Internet-of-Things," *IEEE Trans. Emerg. Top. Comput.*, Vol. 5, No. 4, hal. 586–602, Okt. 2017.

[17] T. Martin, M. Hsiao, Dong Ha, dan J. Krishnaswami, "Denial-of-service Attacks on Battery-powered Mobile Computers," *Proc. of the Second IEEE Annual Conference on Pervasive Computing and Communications*, 2004, hal. 309–318.

[18] F. Stajano dan R.J. Anderson, "The Resurrecting Duckling: Security Issues for Ad-hoc Wireless Network," *Proceedings of the 7th International Workshop on Security Protocols*, 1999, hal. 172–194.

[19] A. Juels, "RFID Security and Privacy: A Research Survey," *IEEE J. Sel. Areas Commun.*, Vol. 24, No. 2, hal. 381–394, Feb. 2006.

[20] M. Lehtonen, D. Ostojic, A. Ilic, dan F. Michahelles, "Securing RFID Systems by Detecting Tag Cloning," *Proc. of 7th International Conference on Pervasive Computing (Pervasive)*, 2009, hal. 291–308.

[21] D.N. Duc dan K. Kim, "Defending RFID Authentication Protocols Against DoS Attacks," *Comput. Commun.*, Vol. 34, No. 3, hal. 384–390, Mar. 2011.

[22] J. P. Walters dan Z. Liang, "Wireless Sensor Network Security : A Survey," dalam *Security in Distributed, Grid, and Pervasive Computing*, Yang Xiao, Eds., New York, USA: Auerbach Publications, CRC Press, 2006, hal. 1–50.

[23] S.W. Boyd dan A.D. Keromytis, "SQLrand: Preventing SQL Injection Attacks," *Appl. Cryptogr. Netw. Secur.*, Vol. 13, No. 10, hal. 292–302, Okt. 2004.

[24] B. Biggio, B. Nelson, dan P. Laskov, "Poisoning Attacks Against Support Vector Machines," *Proc. 29th Int. Conf. Mach. Learn. (ICML 2012)*, 2012, hal. 1-8.

[25] B.I.P. Rubinstein, B.A. Nelson, L. Huang, A.D. Joseph,S.-H. Lau, S. Rao, N. Taft, dan J.D. Tygar, "Stealthy Poisoning Attacks on PCA-based Anomaly Detectors," *ACM SIGMETRICS Perform. Eval. Rev.*, Vol. 37, No. 2, p. 73, 2009.

[26] A.N. Nowroz, K. Hu, F. Koushanfar, dan S. Reda, "Novel Techniques for High-sensitivity Hardware Trojan Detection Using Thermal and Power Maps," *IEEE Trans. Comput. Des. Integr. Circuits Syst.*, Vol. 33, No. 12, hal. 1792–1805, 2014.

[27] M. Msgna, K. Markantonakis, D. Naccache, dan K. Mayes, "Verifying Software Integrity in Embedded Systems: A Side Channel Approach," *Int. Workshop on Constructive Side-Channel Analysis and Secure Design*, 2014, hal. 261–280.

[28] J. P. Walters dan Z. Liang, "Wireless Sensor Network Security : A Survey," dalam *Security in Distributed, Grid, and Pervasive Computing*, Yang Xiao, Eds., New York, USA: Auerbach Publications, CRC Press, 2006, hal. 1–50.

[29] P. Peris-Lopez, J.C. Hernandez-Castro, J.M. Estevez-Tapiador, dan A. Ribagorda, "RFID Systems: A Survey on Security Threats and Proposed Solutions," *Proc. of IFIP TC6 11th International Conference on Personal Wireless Communications*, 2006, hal. 159–170.

[30] J.-J. Quisquater dan D. Samyde, "ElectroMagnetic Analysis (EMA): Measures and Counter-measures for Smart Cards," *Proc. of International Conference on Research in Smart Cards*, 2001, hal. 200–210.

[31] C. Karlof dan D. Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures," *J. Ad-hoc Netw.*, Vol. 1, No. 2, hal. 293–315, 2003.

[32] R. Bonetto, N. Bui, V. Lakkundi, A. Olivereau, A. Serbanati, dan M. Rossi, "Secure Communication For Smart IoT Objects: Protocol Stacks, Use Cases and Practical Examples," *2012 IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM)*, 2012, hal. 1–7.

[33] S. Raza, L. Wallgren, dan T. Voigt, "SVELTE: Real-time Intrusion Detection in the Internet of Things," *Ad Hoc Networks*, Vol. 11, No. 8, hal. 2661–2674, 2013.

[34] J. Daemen dan V. Rijmen, *The Design of Rijndael: Advanced Encryption Standard*, Berlin, Germany: Springer Berlin Heidelberg, 2002.

[35] M. Bellare, A. Desai, E. Jokipii, dan P. Rogaway, "A Concrete Security Treatment of Symmetric Encryption," *Proceedings 38th Annual Symposium on Foundations of Computer Science*, 2002, hal. 394–403.

[36] E.R. Naru, H. Saini, dan M. Sharma, "A Recent Review on Lightweight Cryptography in IoT," *Proc. Int. Conf. IoT Soc. Mobile, Anal. Cloud, I-*

SMAC 2017, 2017, hal. 887–890.

[37] T. Shirai, K. Shibutani, T. Akishita, S. Moriai, dan T. Iwata, "The 128-Bit Blockcipher CLEFIA (Extended Abstract)," *Proc. of International Workshop on Fast Software Encryption*, 2007, hal. 181–195.

[38] A. Bogdanov, L.R. Knudsen, G. Leander, C. Paar, A. Poschmann, M.J.B. Robshaw, Y. Seurin, dan C. Vikkelsoe, "PRESENT: An Ultra-Lightweight Block Cipher," *Proc. of International Workshop on Cryptographic Hardware and Embedded Systems*, 2007, hal. 450–466.

[39] R. Kumar dan S. Rajalakshmi, "Mobile Sensor Cloud Computing: Controlling and Securing Data Processing Over Smart Environment through Mobile Sensor Cloud Computing (MSCC)," *Proceedings - 2013 International Conference on Computer Sciences and Applications, CSA 2013*, 2013, hal. 687–694.

[40] S. Misra dan A. Vaish, "Reputation-based Role Assignment for Role-based Access Control in Wireless Sensor Networks," *Comput. Commun.*, Vol. 34, No. 3, hal. 281–294, 2011.

[41] H. Mouratidis dan P. Giorgini, "Security Attack Testing (SAT)-Testing the Security of Information Systems at Design Time," *Inf. Syst.*, Vol. 32, No. 8, hal. 1166–1183, 2007.

[42] B.I.P. Rubinstein, B. Nelson, L. Huang, A.D. Joseph, S.-H. Lau, S. Rao, N. Taft, dan J.D. Tyga, "ANTIDOTE: Understanding and Defending Against Poisoning of Anomaly Detectors," *Proceedings of the 9th ACM SIGCOMM Conference on Internet Measurement Conference - IMC '09*, 2009, hal. 1-14.

[43] M. Mozaffari-Kermani, S. Sur-Kolay, A. Raghunathan, dan N. K. Jha, "Systematic Poisoning Attacks on and Defenses for Machine Learning in Healthcare," *IEEE J. Biomed. Heal. Informatics*, Vol. 19, No. 6, hal. 1893–1905, 2015.

[44] M. Kumar (2016) "How to Hack WiFi Password from Smart Doorbells," [Online], https://thehackernews.com/2016/01/doorbell-hacking-wifi-pasword.html, tanggal akses: 12-Agu-2019.

[45] A. Chapman (2014) "Hacking into Internet Connected Light Bulbs," [Online], https://www.contextis.com/en/blog/hacking-into-internet-connected-light-bulbs, tanggal akses: 12-Agu-2019.

[46] J. Liu, Y. Wang, G. Kar, Y. Chen, J. Yang, dan M. Gruteser, "Snooping Keystrokes with mm-level Audio Ranging on a Single Phone," *Proc. 21st Annu. Int. Conf. Mob. Comput. Netw.*, 2015, hal. 142–154.

[47] L. Lu, J. Yu, Y. Chen, Y. Zhu, X. Xu, G. Xue, dan M. Li, "KeyListener: Inferring Keystrokes on QWERTY Keyboard of Touch Screen Through Acoustic Signals," *IEEE INFOCOM 2019 - IEEE Conference on Computer Communications*, 2019, hal. 775–783.

[48] E. McKenna, I. Richardson, dan M. Thomson, "Smart Meter Data: Balancing Consumer Privacy Concerns with Legitimate Applications," *Energy Policy*, Vol. 41, hal. 807–814, 2012.

[49] Y. Michalevsky, G. Nakibly, A. Schulman, G.A. Veerapandian, dan D. Boneh, "PowerSpy: Location Tracking using Mobile Device Power Analysis," *SEC'15 Proceedings of the 24th USENIX Conference on Security Symposium*, 2015, hal. 785–800.