UAS

Survey Tentang Keamanan *Internet of Thinks*

Toni Tri Atmojo [1], Eko Dian Savutra [2], M.Ardi Wiratama Putra [3]
Magister Teknik Informatika, Universitas Bina Darma [1,2,3]
toni.triatmojo@binadarma.ac.id [1]
eko.diansavutra@binadarma.ac.id [2]
ardiewitra@gmail.com [3]

Abstrak

Internet of Things (IoT) adalah suatu konsep atau program dimana sebuah objek memiliki kemampuan untuk mentransmisikan atau mengirimkan data melalui jaringan tanpa menggunakan bantuan perangkat komputer dan manusia Teknologi *IoT* diharapkan dapat membuka jalan bagi aplikasi inovatif di berbagai bidang seperti keamanan dan pengawasan, transportasi, dan industri, serta mengintegrasikan teknologi komunikasi yang canggih, jaringan, komputasi awan, dan penginderaan. Mengingat banyaknya perangkat terhubung yang berpotensi rentan risiko yang sangat signifikan muncul seputar masalah keamanan, privasi, dan tata kelola. Aplikasi *IoT* diharapkan dapat mempengaruhi banyak aspek kehidupan masyarakat, membawa banyak kemudahan, namun jika keamanan dan privasi tidak dapat dipastikan, hal ini dapat menyebabkan sejumlah danpak yang tidak diinginkan. Dalam penelitian ini, kami menyediakan survei dan klasifikasi menyeluruh dari kerentanan yang ada, serangan yang dapat dieksploitasi, kemungkinan penanggulangan serta mekanisme *control* akses termasuk otentikasi dan otorisasi. Selain itu, pekerjaan ini juga berfokus pada kerentanan intrinsik *IoT* serta tantangan keamanan di setiap lapisan. Serta metode untuk mitigasi risiko, dengan pencegahan dan saran untuk perbaikan dibahas.

Kata Kunci : *Internet of Things (IoT)*, Survey, Keamanan

1. Pendahuluan *(Introduction)*

Pesatnya pertumbuhan dari Teknologi *Internet of Things* berbagai perangkat elektronik yang terhubung ke Internet merupakan bukti yang cukup baik. *Internet of Things (IoT)* mendefinisikan perangkat yang mampu berinteraksi dengan pengguna dan perangkat lain melalui infrastruktur jaringan dengan interaksi pengguna yang terbatas atau tidak ada sama sekali. Dalam beberapa tahun terakhir, konsep seperti *Smart Phone*, *Smart Car*, *Smart City*, dan rumah pintar telah menerima minat besar dari banyak komunitas penelitian yang berbeda. Kombinasi konsep-konsep ini dianggap sebagai masa depan Internet dan disebut *Internet of Things (IoT*).

Keberhasilan implementasi *IoT* memerlukan pertimbangan sejumlah faktor penting termasuk namun tidak terbatas pada teknologi komunikasi, protokol komunikasi, perangkat keras dan perangkat lunak yang disematkan. Aplikasi *IoT* diharapkan dapat mempengaruhi banyak aspek kehidupan masyarakat dan membawa banyak kemudahan, namun jika keamanan dan privasi tidak dapat dipastikan, hal ini dapat menyebabkan sejumlah konsekuensi yang tidak diinginkan. Selain itu, lingkungan *IoT* harus memberikan solusi untuk tantangan lain seperti keandalan, kinerja, ketersediaan, mobilitas, manajemen, interoperabilitas, skalabilitas, dan *Big Data*. Keamanan *IoT* adalah

area perhatian utama, ini adalah tantangan yang paling berdampak bagi *IoT* di lapisan aplikasi. Persyaratan keamanan *IoT* harus disediakan untuk semua lapisan, selain itu, keamanan *IoT* juga harus mencakup keamanan sistem secara keseluruhan di tiga lapisan yang dikenal sebagai keamanan lintas lapisan. Salah satu masalah keamanan yang paling menarik dalam keamanan lintas lapisan *IoT* adalah deteksi dan pencegahan intrusi. Intrusi adalah aktivitas ganas apa pun yang dapat membahayakan integritas, kerahasiaan, atau ketersediaan sumber daya *IoT*. Salah satu tantangan penelitian yang layak dalam jaringan *IoT* adalah mengamankannya dari entitas jahat yang melakukan aktivitas rentan (ancaman atau serangan). Ada banyak serangan yang mengancam sumber daya *IoT*, di antaranya penolakan layanan *(DoS)* semakin populer dengan variannya penolakan layanan terdistribusi *(DDoS)*. *DDoS* adalah serangan yang mencoba oleh node jahat untuk mengganggu sumber daya atau *bandwidth* pengguna yang sah ketika ditembus dari berbagai *node* yang disusupi. Serangan *DoS* yang meliputi membanjiri sejumlah besar lalu lintas untuk menempati sumber daya jaringan, *bandwidth*, target waktu *CPU*. Serangan *DoS* yang paling umum adalah siaran *ICMP*, banjir *SYN*, banjir *Ping*, banjir *DNS*, banjir *UDP* dan sebagainya. Serangan *DDoS* dapat terlibat di setiap lapisan *IoT* tiga lapisan seperti serangan *jamming* yang ada di lapisan sensor atau fisik, Serangan Banjir di lapisan jaringan dan pemrograman ulang dan Serangan *DDoS* berbasis jalur ada di lapisan aplikasi.

Dalam bab ini, kami menyediakan survei dan klasifikasi menyeluruh dari kerentanan yang ada, serangan yang dapat dieksploitasi, kemungkinan penanggulangan serta mekanisme *control* akses termasuk otentikasi dan otorisasi. Selain itu, pekerjaan ini juga berfokus pada kerentanan intrinsik *IoT* serta tantangan keamanan di setiap lapisan. Serta metode untuk risiko, dengan pencegahan dan saran untuk perbaikan dibahas.

2. Metode Tinjauan Pustaka *(Literature Review Method)*

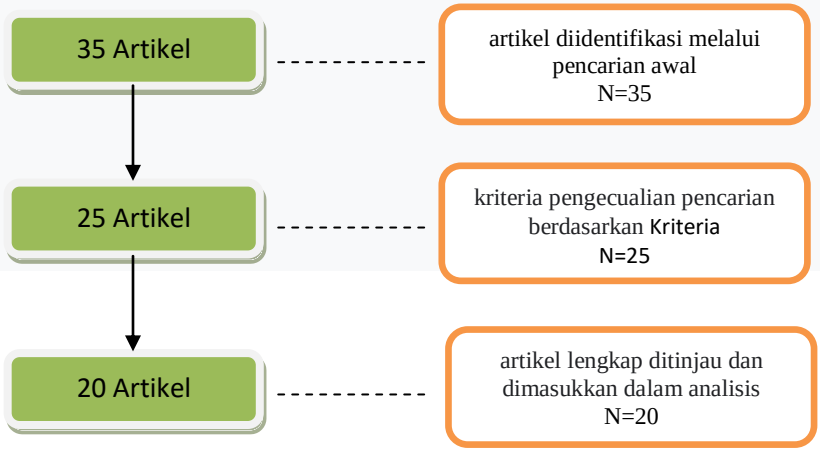
Metode Tinjauan Pustaka ini dilakukan dengan menggunakan pendekatan *literature review*. Tinjauan pustaka merupakan salah satu tahapan terpenting dalam kegiatan penelitian, di mana hal ini akan menjadi dasar yang kuat untuk mengetahui keadaan seni perkembangan teknologi dan sistem informasi. Dalam penelitian ini, ada empat tahap dari tinjauan literatur. Tahap pertama adalah meninjau tujuan dan protokol penelitian. Tahap kedua adalah untuk melakukan pencarian *literature* dan melakukan penyaringan setiap artikel dengan kata kunci *Survey* Tentang Keamanan *Internet of Thinks*. Tahap ketiga menilai kualitas artikel dan ekstraksi data. Akhirnya, keempat tahap adalah menganalisis temuan.

2.1. Tahap Perencanaan *(Planing Phase)*

Tahap pertama yaitu meninjau tujuan dan protokol, merupakan elemen penting yang harus dilakukan dalam tinjauan literature Protokol peninjauan dapat mengurangi dalam rencana penelitian. Tahapan ini membahas tentang tujuan dari *literature review* dan desain protokol dan kriteria literatur, metode ekstraksi data, analisis data, dan presentasi hasil *review*.

2.2. Tahap Seleksi *(Selection Phase)*

Pada *review* tahap kedua, artikel ilmiah di*review* artikel ilmiah dalam *database Google Scolar* dari 2016-2020. Artikel ilmiah diambil sebagai bahan *review* adalah artikel yang berhubungan dengan topik *review* yaitu *Survey* Tentang Keamanan *Internet of Thinks.* Kerangka waktu yang digunakan untuk pencarian artikel ini dipilih karena relatif teknologi baru. Pencarian artikel dilakukan dalam berbagai jenis seperti makalah jurnal, Dalam mencari artikel yang sesuai dengan tujuan yang telah ditentukan, kami menggunakan kata kunci menggunakan Keamanan *Internet of Thinks.* Setelah mendapatkan hasil, dilakukan proses penyaringan untuk memastikan artikel yang diperoleh adalah artikel yang sesuai. Proses penyaringan ini dilakukan dengan membuang artikel yang tidak relevan dengan topik dan studi tentang Keamanan *Internet of Thinks*, Dari proses awal ini, kami memperoleh 35 makalah. Lihat Gambar 1 di bawah ini, yang menunjukkan proses pemilihan artikel.



Gambar 1. Pemilihan Artikel Berdasarkan Pencarian Angka

2.3. Kriteria Eksklusi dan Inklusi *(Exclusion and Inclusion Criteria)*

Pada Tahap 3 dilakukan pemilihan artikel dengan kriteria eksklusi. Tahap ini menghilangkan artikel yang tidak sesuai atau tidak relevan dengan topik penelitian, menghapus artikel yang tidak menyediakan artikel yang lengkap, menghapus artikel yang tidak dapat diunduh atau diakses, dan menghapus artikel yang tidak diterbitkan antara 2016–2020. Kemudian, tahap ini juga menghapus artikel yang tidak terkait dengan *Survey* Tentang Keamanan *Internet of Thinks*. Setelah pengecualian proses dilakukan, langkah selanjutnya adalah memilih kriteria inklusi, yaitu makalah jurnal, dan artikel yang cocok dengan kriteria inklusi mengenai *Survey* Tentang Keamanan *Internet of Thinks.*

2.4. Perpaduan *(Syntesis)*

Tahap akhir dari *review* ini adalah mengekstrak data atau informasi dari artikel yang akan digunakan sebagai bahan kajian, analisis dan identifikasi *Survey* Tentang Keamanan *Internet of Thinks* . Pada tahap ini, ekstraksi dilakukan dengan menggunakan metode kualitatif. Analisis data dilanjutkan dengan studi *literature review* laporan.

3. Framework dan *Survey* Keamanan *Internet of Thinks*

3.1. Privasi dan Keamanan

Serangan baru pada struktur *IoT* menghadirkan sistem keamanan lengkap untuk melindungi sistem dan informasi dari ujung ke ujung. Serangan ancaman yang mengeksploitasi kelemahan pada perangkat individu untuk memasuki struktur dan mengakses *gadget* yang lebih aman dari luar merupakan inspirasi pendorong untuk solusi keamanan yang lengkap. Ini termasuk penelitian teknik kriptografi yang baik untuk keamanan sistem dan data, teknik *non-kriptografi* untuk keamanan dan kerangka kerja membantu pengembang untuk mengembangkan sistem yang aman pada perangkat *heterogen* dengan lebih mudah. Solusi keamanan *kriptografi* yang cocok untuk dijalankan pada perangkat *IoT* dengan sumber daya terbatas, kami memerlukan penelitian untuk mengaktifkan pengguna dari semua tingkat kemampuan untuk mengirim dan menggunakan sistem *IoT* dengan aman meskipun antarmuka pengguna terbatas yang dapat diakses dengan sebagian besar *gadget IoT.*

3.2. *Taksonomi* Keamanan *IoT*

Taksonomi yang kami usulkan disajikan yang menguraikan struktur lengkap arsitektur *IoT* dari lapisan dan levelnya hingga berbagai teknologi dan tujuan keamanannya, diikuti oleh ancaman keamanan di setiap level. Penting untuk dicatat

bahwa klasifikasi keamanan yang dibahas dikategorikan ke dalam kombinasi lapisan arsitektur dan teknologi *IoT*. Pada lapisan informasi, tanpa memperhatikan kebutuhan akan privasi dan otorisasi pengguna dan data, jaringan *IoT* dapat menghadapi masalah keamanan seperti *jamming, eavesdropping*, dan *spoofing*. Semua serangan ini memblokir sinyal dari transmisi/penerimaan, dapat menyebabkan perulangan dan memungkinkan penyusup yang tidak berwenang untuk menangkap data atau menghasilkan pesan kesalahan palsu yang dapat mengubah target perutean.

3.3. *Learing Methods for IoT Security*

Metode pembelajaran untuk keamanan *IoT* telah dikelompokkan ke dalam *ML*, metode *DL* dan *RL*. Metode *ML* terdiri dari diawasi dan pendekatan tanpa pengawasan. Pendekatan yang diawasi adalah yang dikategorikan lebih lanjut menjadi *DT, SVM, NB, KNN, RF, AR* dan *EL*. Selain itu, metode tanpa pengawasan hanya terdiri dari dua metode, yaitu *K-Means* dan *PCA*. Metode *DL* juga dikelompokkan menjadi pendekatan terawasi, tidak terawasi, dan hibrida. Pendekatan terbimbing terdiri dari metode *AE, RBM,* dan *DBN*. Terkahir penedekatan hybrid terdiri dari *GAN* dan metode *EDLN*. Tidak ada kategori lebih lanjut yang ditemukan di bawah metode *RL*.

3.4. Lapisan Sesi

Menurut sebagian besar peneliti, arsitektur tiga lapis *IoT* tidak mengakomodasi pembukaan, penutupan, dan pengelolaan sesi antara dua hal. Oleh karena itu, diperlukan suatu protokol yang dapat mengatasi permasalahan tersebut dan dapat mempermudah komunikasi antar perangkat. Lapisan sesi abstrak harus diakomodasi sebagai lapisan tambahan dalam arsitektur *IoT* yang secara khusus dapat mengelola koneksi, protokol, dan sesi antara perangkat *heterogen* yang berkomunikasi.

Tabel 1. *Framework dan Survey Keamanan Internet of Thinks*

No	Tahun Publikasi	Tujuan Keamanan	Masalah	Tantangan
1	2020	*Security and Privacy*	Kekurangan Algoritma privasi dan keamanan yg efisien.	Memastikan informasi pribadi mereka sebagai lawan dari mengharapkan komponen *actual* dalam kerangka *IoT* dalam menjaga privasi mereka.
2	2020	*Survey and taxonomy*	Menangani tidak hanya masalah keamanan, tetapi juga mengingat ancaman	Model masa depan seharusnya tidak hanya

			lingkungan, biaya per pengguna, kemudahan skalabilitas, dan latensi layanan di jaringan *IoT*.	menangani masalah keamanan data dan privasi dalam kerangka kerja *IoT* tetapi juga konsumsi daya yang tinggi, latensi layanan, desentralisasi data, dan pengeluaran keuangan yang besar
3	2020	*Survey Machine deep Learning Methods*	Serangan "Mirai" adalah jenis botnet yang baru baru ini menyebabkan serangan DDoS skala besar dengan mengekspoitasi perangkat IoT	Persayaratan untuk mengamankan IoT telah menjadi kompleks karena beberapa teknologi, dari perangkat fisik dan transmisi nirkabel ke arsitektur seluler dan cloud, perlu diamankan dan dikombinasikan dengan teknologi lain.
4.	2016	*Environment Survey; Traffic and QoS*	Banyak responden mengungkapkan kecemasan mereka atas meningkatnya jumlah kerentanan *IoT* dan merasa bahwa mereka akan menjadi bencana jika langkah-langkah keamanan yang tepat tidak diberlakukan.	masalah yang dihadapi dalam penyebaran *IoT* di Cina dan mengusulkan arsitektur terbuka tiga lapis untuk mengatasi tantangan ini

4. Kesimpulan

IoT Diharapkan dapat mengintegrasikan teknologi komunikasi, jaringan, komputasi awan, dan penginderaan yang akan mempengaruhi banyak aspek di kehidupan masyarakat dan banyak membawa kemudahan. Namun demikian, mengingat sejumlah besar perangkat terhubung ke internet sangat berpotensi rentan akan resiko yang di dapatkan. Kami membahas tantangan saat ini terkait dengan penyediaan privasi yang merupakan komponen penting, karena tanpa keamanan yang cukup, teknologi ini tidak akan berguna dan hanya akan membahayakan manusia. *Survey* ini berfokus pada masalah dan tantangan keamanan *IoT*, menyajikan gambaran umum tentang solusi keamanan *IoT* terkini dan menyajikan beberapa tantangan terbuka di bidang ini,