Data Privasi dan Keamanan Siber pada *Smart-City*: Tinjauan Literatur

Dyah Ayu Suci Ilhami
Program Studi Magister Informatika
Universitas Islam Indonesia
Yogyakarta, Indonesia
21917027@students.uii.ac.id

***Abstract*—Perkembangan teknologi yang semakin canggih dari tahun ke tahun sehingga membuat digitalisasi menjadi perbincangan utama. Maka dari itu sistem dalam sebuah kabupaten maupun kota juga harus menerapkan digitalisasi. *Smart-City* merupakan suatu gerakan yang digencarkan oleh pemerintah dalam rangka menerapkan sistem digital di beberapa kota dan kabupaten, tentunya termasuk dengan infrastrukturnya. Namun, dikarenakan rancangan ini masih tahap awal dari 2017, perlu dipertimbangkan beberapa teknologi agar ketika sebuah kabupaten ataupun kota ingin menjadi *Smart-City*, tingkat keamanan, privasi data, dan semacamnya tetap terjamin keamanannya. Artikel tinjauan literatur ini menggunakan metode systematic literature review atau SLR, dimana digunakan sebanyak 20 artikel yang telah membahas topik ataupun objek yang sama. Berdasarkan hasil dari metode SLR terdapat beberapa teknologi yang dapat membantu sistem keamanan dan perlindungan data privasi masyarakat ataupun pemerintah, salah satunya menggunakan teknologi IoT. Penerapan IoT di negara lain sudah memperlihatkan hasil yang cukup memuaskan, sehingga layak jika diterapkan di Indonesia. Kesimpulan artikel ini menunjukkan bagaimana arsitektur IoT dan blockchain mampu melindungi keamanan dan privasi data; serta teknologi apa saja yang perlu digunakan untuk menyeimbangkan dengan program atau gerakan *Smart-City*.**

***Kata Kunci*—Keamanan Siber, Privasi Data, Smart-City, IoT**

I. PENDAHULUAN

Gerakan kota pintar atau yang sering dikenal dengan istilah *Smart-City* sedang digencar-gencarkan oleh pemerintah sejak 2017 untuk diterapkan pada kota atau kabupaten yang berada di Indonesia. Gerakan menuju 100 *Smart-City* yang dilakukan oleh pemerintah supaya dapat membimbing kota atau kabupaten agar lebih memaksimalkan penggunaan dan pemanfaatan teknologi sesuai era digitalisasi dan juga diharapkan dapat meningkatkan pelayanan masyarakat sesuai dengan potensi dan kapasitas kabupaten atau kota nya masing-masing. Selain dengan penerapan teknologi, jika sebuah kabupaten atau kota akan menerapkan *Smart-City* juga harus melengkapi infrastruktur dasar, harus memiliki transporatasi yang terintegrasi dan efisien, penduduk atau talenta yang cerdas atau *Smart* people dan perkembangan ekonomi yang stabil pengeluaran dan pemasukannya atau *Smart economy* [1]. Untuk penerapannya sendiri, di Indonesia pada tahun 2022 sudah ada 191 dari 514 kabupaten kota yang berada di Indonesia, namun akan ada penambahan pada tahun 2022 ini dengan menambahkan target sebanyak 50 kabupaten atau kota yang terpilih [2]. Untuk penerapan sistem *Smart-City* di Indonesia sendiri tidak boleh asal membuat suatu kabupaten menjadi *Smart-City* namun harus memperhatikan beberapa elemen dan enam komponen ataupun infrastruktur agar kabupaten ataupun kota saat diterapkan *Smart-City* seluruh aktivitas dapat berjalan dengan normal, sistem keamanan dan perlindungan data privasi tidak menjadi masalah, dan juga mampu menyiptakan keyakinan kepada masyarakat dengan penerapan *Smart-City* di kabupaten ataupun kotanya, lihat Gambar 1.

Elemen-elemen tersebut diperkuat pada sisi keamanannya termasuk elemen open data yang banyak menyimpan data privasi penggunanya, dan juga karena seluruh elemen mengandalkan sistem cerdas maka harus diketahui juga bagaimana tantangan keamanan siber dalam penarapan *Smart-City* pada kabupaten ataupun kota. Beberapa tantangan point yang perlu diperhatikan dalam penerapan *Smart-City* sudah dijabarkan dalam beberapa penelitian. Tantangan dan point dalam penerapan *Smart-City* menjadi salah satu hal yang menarik untuk dibahas lebih jauh terutama jika tantangan dan solusinya dapat diterapkan dalam kabupaten maupun kota di Indonesia. Beberapa penelitian terdahulu banyak yang menjabarkan mengenai point tersebut seperti, penelitian yang dilakukan oleh Alamer menyatakan bahwa jika sistem cerdas ini diterapkan dalam beberapa kota di Indonesia maka akan rentan terhadap peretasan data dan penyerangan dalam dunia maya jika kebutuhan keamanan tidak mendukung. Maka dari itu, dalam penelitiannya menyarankan mitigasi terbaik dalam hal keamanan siber dan data privasi menggunakan keamanan siber yang berbasis dengan data besar atau big data, dapat juga menggunakan teknologi yang dinamakan blockchain [3]. Penelitian yang kedua, yang dilakukan oleh Alshambri, yang menyatakan bahwa infrastruktur global untuk menyalurkan informasi kepada masyarakat secara meluas dan canggih di masa yang akan datang yakni menggunakan teknologi IoT atau Internet of Things. Karena teknologi IoT merupakan hasil kombinasi dan pengembangan dari beberapa teknologi sebelumnya dan IoT ini juga sudah bisa mencangkup untuk kebutuhan sistem pada *Smart-City*,

Gambar 1. Elemen Penting dalam Penerapan *Smart-City*

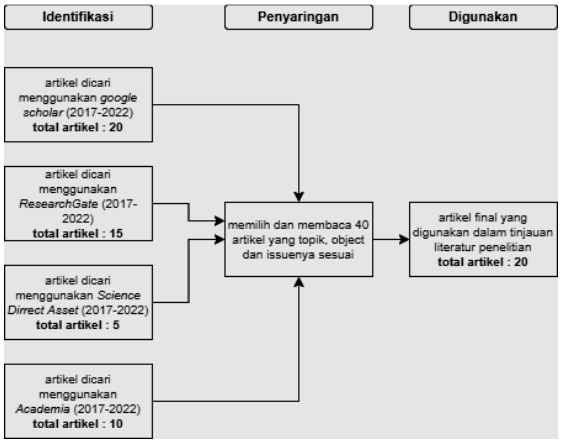
namun selain IoT dalam penerapan *Smart-City* juga membutuhkan beberapa teknologi besar lainnya seperti teknologi blockchain, big data, dan cloud computing. Namun, penggunaan IoT hanya akan tercapai hasilnya dengan sempurna apabila sistem keamanan siber yang diterapkan juga sudah baik supaya teknologi IoT tidak dapat teretas, terakses ataupun teredit secara sembarang orang. Dan untuk menerapkan keamanan siber yang bagus maka ada beberapa tantangan, simulasi serangan dan bagaimana cara mencegahnya [4].

Dengan adanya beberapa penelitian terdahulu yang membahas topik dan pembahasan yang sama. Maka dalam artikel ini akan membahas apakah seluruh kabupaten ataupun kota yang sudah menerapkan sistem *Smart-City* sudah memenuhi seluruh infrastruktur menjadi kota cerdas terutama di negara Indonesia, bagaimanakah dengan data-data yang tersimpan dahulu apakah setelah berpartisipasi dan masuk kedalam gerakan *Smart-City* data privasi tetap aman secara keseluruhan dan bagaimana mengenai tingkat keamanan terutama dalam menghapi kejahatan dunia maya apakah sudah cukup memadahi dan melindungi orang maupun data di dalamnya dan juga bagaimanakan anggaran yang dikeluarkan apakah negara atau pemerintah mampu mengeluarkan dana besar demi keamanan ataupun teknologi yang semakin canggih untuk keperluan *Smart-City*. Jika dilihat dari kabupaten ataupun kota yang sudah menerapkan gerakan *Smart-City* pada tahun 2022, terdapat peningkatan pasar IoT di Indonesia yaitu sebesar Rp355,2 triliun, lalu di beberapa kota sudah terdapat beberapa program *Smart-City* yang dapat dinikmati oleh masyarakat seperti program War Room, layanan homecare, layanan LOPIS dan masih banyak lainnya [5].

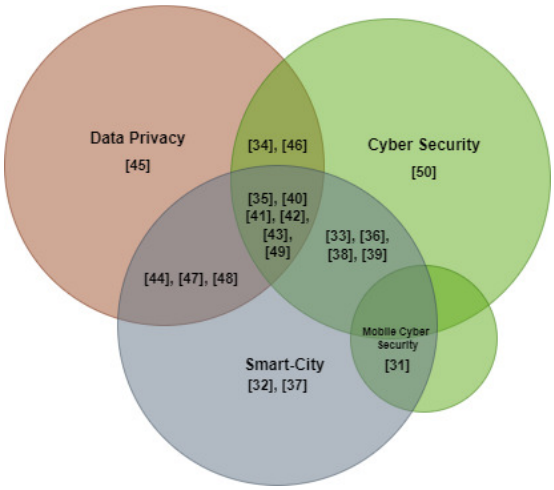
Oleh karena itu, pada bagian analisa dan pembahasan akan menjabarkan mengenai bagaimana tingkat keamanan kabupaten atuapun kota yang sudah menerapkan *Smart-City* baik dalam kejahatan dunia siber ataupun keamanan dalam pengamanan data privasi negara. Sehingga, akan jelas kelihatan dimana posisi yang harusnya dapat lebih ditingkatkan ataupun hal yang dapat dikurangi demi menyukseskan sistem *Smart-City* terutama dalam sisi keamanannya.

II. REVIU LITERATUR

Teori diambil melalui beberapa jurnal dari beberapa macam search engine nasional maupun international seperti



Gambar 2. Diagram Alir Tinjauan Literatur



Gambar 3. Treemap Ringkasan Tinjauan Literatur

Google Scholar, ResearchGate, Science Dirrect Assets, dan Academia dengan yang ditinjau berfokus pada topik dan objek yang akan digunakan dalam penelitian. Untuk melihat proses penyaringan jurnal dapat dilihat pada Gambar 2.

Hasil yang digunakan sesuai pada Gambar 2 akan dibahas dan diidentifikasi dalam point 3. Diluar dari Gambar 2 terdapat beberapa jurnal pendukung untuk mencari teknologi-teknologi apa saja yang mampu menyeimbangkan sistem *Smart-City* yang akan diterapkan seiring perkembangan teknologi yang semakin canggih. Selain diagram alir, dalam artikel penelitian juga menyediakan treemap ringkasan dari tinjauan literatur yang digunakan agar jelas tinjauan literatur sebelumnya jika dipadukan dengan penelitian saat ini memiliki kesamaan dibidang objek, topik, atau permasalahannya. Treemap ringkasan tinjauan literatur selanjutnya dapat dilihat pada Gambar 3. Dalam treemap nantinya akan terbagi menjadi 3 point utama yaitu data privacy, cyber security dan *Smart-City*, setelah dibagi menjadi 3 point utama, jurnal jurnal referensi sebelumnya akan dimasukan sesuai dengan topik, pembahasan atau permasalahan yang sama.

Jika dilihat pada Gambar 3, jurnal atau artikel yang banyak digunakan dalam penelitian sudah mencangkup ketiga objek penting yaitu privasi data atau data privacy, keamanan siber atau cyber security dan terakhir kota pintar atau *Smart-City*. Sehingga, pembahasan, hasil dan analisa pada point point berikutnya yang berasal dari jurnal jurnal ini sudah mencangkup secara keseluruhan dalam topik dan permasalahan yang akan dibahas.

A. Smart-City

Teknologi yang semakin maju membuat pemerintah Indonesia ingin meningkatkan sistem pada kabupaten ataupun kota agar bergerak ke arah digitalisasi dengan teknologi dan sumber daya yang mewadahi. Untuk saat ini di Indonesia sudah lebih dari 100 kabupaten atau kota yang mengikuti gerakan *Smart-City* namun, yang perlu diperhatikan ketika kabupaten atau kota lain ingin menerapkan dan mengikuti *Smart-City* sektor lain seperti transportasi, kesehatan, layanan pemerintah, eneri, masyarakat juga harus sudah mulai diperhatikan bagaimana akan perkembangannya bagaimana akan kesiapan menghadapi gerakan *Smart-City* [6].

Gambar 4. Infrastruktur *Smart-City* di Indonesia

Adapula beberapa pengertian kota cerdas atau *Smart-City* yang sudah diungkapkan oleh beberapa ahli, seperti pengertian pertama yakni sebuah kota yang sudah memiliki rencana untuk meningkatkan performancenya namun dapat mengurangi konsumsi ataupun biaya yang dikeluarkan serta berencana terlibat secara aktif, efektif dan efisien kepada seluruh warganya menggunakan bantuan teknologi yang amat canggih. Ataupun pengertian kedua yang menjelaskan *Smart-City* itu sebuah visi dan misi dalam bentuk pengembangan sebuah kota atau kabupaten dengan tujuan menyukseskan integrasi teknologi yang dimiliki termasuk teknologi IoT secara benar dan aman untuk penggunaannya mengelola dan mengatur kabupaten atau kota [7].

Selain pengertian dan tujuan yang penting dalam penerapan *Smart-City* pada beberapa kabupaten ataupun kota, disini juga harus mempertimbangkan infrastruktur infrastruktur yang harus dimiliki sebuah kabupaten agar dapat mengikuti gerakan *Smart-City* ini seperti yang ada pada Gambar 4. Terdapat enam infrastruktur terutama pada kabupaten atau kota yang memiliki banyak kawasan kabupaten atau kota [8]:

1. Lingkungan yang cerdas atau *Smart* environment, yang mana setiap kabupaten ataupun kota yang memiliki kawasan wisata lebih banyak mampu menjaga lingkungannya yang bersih bebas akan sampah dan selalu menjaga seni tradisional dari kawasan tersebut.
2. Eknomi yang cerdas atau *Smart economy*, yang sudah menerapkan sistem transaksi cashless lebih banyak di semua kabupaten ataupun kota namun prioritasnya adalah kabupaten atau kota yang memiliki banyak kawasan wisata.
3. Pencitraan merk yang cerdas atau *Smart* branding, yang jika diterapkannya *Smart-City* didaerahnya akan tetap mampu membantu pemerintah daerah dalam meningkatkan atau memasarkan produk dan wisata dari daerah kabupaten ataupun kota tersebut.
4. Sistem pemerintahan yang cerdas atau *Smart* government, sebelum kabupaten ataupun kota menerapkan gerakan *Smart-City* maka harus dipastikan terlebih dahulu apakan pemerintahannya sudah menerapkan sistem yang berbasis elektronik atau yang dikenal dengan nama SPBE dengan kualitas dan pelayanan terhadap publik yang baik dan mumpuni.
5. Masyarakat yang cerdas atau *Smart* society, sebelum terselenggarakannya suatu kabupaten ataupun kota sebagai *Smart-City* maka harus memastikan terlebih dahulu terutama pada kabupaten ataupun kota yang memiliki kawasan wisata lebih banyak, apakah masyarakat disana sudah memiliki kapasitas yang banyak dan bagaimana sikap masyarakat pada daerah tersebut jika menjadi tuan rumah banyak wisatawan datang ke daerahnya
6. Hidup cerdas atau *Smart* living, hidup cerdas ini sangat penting jika suatu kabupaten ataupun kota ingin menerapkan sistem *Smart-City* karena harus memastikan dahulu bagaimana situasi atau keadaan lingkungan bagi para wisatawan, apakah transportasi dan bahan pangan menyukupi, aman dan ramah.

Untuk melengkapi teori-teori yang dapat memperkuat artikel dalam poin *Smart-City*, menggunakan beberapa artikel terdahulu yang bisa dicari dengan beberapa kata kunci, seperti: *Smart-City*, infrastruktur, teknologi IoT, komponen *Smart-City*.

B. Keamanan Siber

Keamanan siber atau cyber security yang saat saat ini sering diperbincangkan banyak orang terutama seiring kemajuan teknologi yang semakin lama semakin canggih. Teknologi yang semakin canggih maka keamanan dalam teknologi juga seharusnya lebih diperketat apalagi sekarang makin banyak aktivitas yang dilakukan dalam dunia maya atau cyberspace. Ada beberapa definisi mengenai keamanan siber yang diperbincangkan ramai orang, salah satu definisinya yaitu sebuah tindakan untuk mengukur dan memastikan keamanan barang, alat maupun aset terhadap resiko-resiko keamanan yang berkaitan dengan barang tersebut pada kejahatan di dunia maya [9].

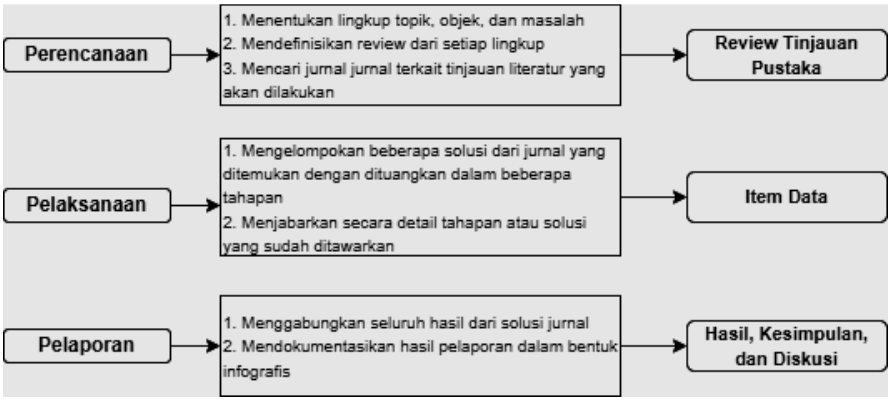
Jika dilihat dan ditinjau dengan penerapannya dalam pemerintah Indonesia terutama dalam gerakan *Smart-City*, resiko dalam pengamanan siber sangat berpengaruh terhadap perwujudan penerapan dan keunggulan di masing – masing kabupaten ataupun kota. Ada beberapa ancaman keamanan siber jika diterapkan dalam gerakan *Smart-City* seperti ancaman keamanan terhadap sistem *Smart-City* secara langsung dan ada juga ancaman keamanan terhadap jaringan yang akan digunakan dalam gerakan *Smart-City* yang pastinya terdiri dari bermacam – macam ancaman dan kontrol didalamnya [3].

Tanpa dipasang atau diterapkannya keamanan siber dalam sebuah kegiatan ataupun aktivitas yang banyak dilakukan dalam dunia maya maka, kegiatan atau aktivitas tersebut tidak dapat mempertahankan diri terhadap peretasan yang digencarkan oleh hacker, pelanggaran data dan pastinya akan sering menjadi sasaran target selanjutnya bagi penyerang hacker [10].

Untuk melengkapi teori-teori yang dapat memperkuat artikel dalam poin keamanan siber, menggunakan beberapa artikel terdahulu yang bisa dicari dengan beberapa kata kunci, seperti: security, cyberspace, ancaman kejahatan cyber, ancaman keamanan.

C. Data Privasi

Data privasi atau informasi yang bersifat bukan umum dalam artian hanya beberapa orang saja yang mendapatka



Gambar 5. Metodologi Literatur Review (SLR)

akses jika dalam masa sekarang merupakan salah satu hal yang penting yang dapat menentukan perkembangan sebuah organisasi yang dipimpin, tetapi karena teknologi yang semakin canggih maka keamanan data privasi akan menjadi salah satu hal yang menjadi ancaman terbesar karena peretasan dan pembocoran data sudah banyak dilakukan oleh para hacker [11]. Perlindungan data jika sudah masuk dalam dunia teknologi biasa disebut dengan metodologi keamanan sebuah komputer. Terdapat beberapa jenis keamanan jika menyangkut privacy data yang tidak bisa dianggap sepele, seperti keamanan data saat mendownload aplikasi, keamanan data yang ada pada komputer, keamanan data pada jaringan terutama jika data dan jaringan dalam skala besar, dan masih banyak lagi jenis – jenis keamanan lainnya [12].

Dan jika dinilai bagaimana perlindungan data privasi sendiri di Indonesia, jika melihat dari Undang – Undang yang ada untuk perlindungan data privasi belum ada UU dan kebijakan secara khusus, jadi masih tergabung dalam ayat ayat di UU. Namun, jika ingin menelisik mengenai UU ITE untuk perlindungan privacy data dalam sebuah sistem elektronik dapat masuk ke dalam UU ITE No. 19 Tahun 2016 yang meliputin perlindungan data privasi dari penyelenggaran sistem dan penggunaan tanpa izin. Untuk lebih detail bisa melihat Pasal 26 ayat 1 dalam UU ITE No. 19 Tahun 2016 yang menjelaskan lebih jauh mengenai apa saja hak yang didapatkan oleh pribadi seseorang.

Secara singkat penjelasan dari pasal tersebut yaitu, perlindungan data privasi merupakan salah satu bagian dari hak pribadi yang semua orang berhak memiliki baik dalam pemanfaatan teknologi informasi ataupun diluar teknologi informasi. Maka dari itu, jika terdapat seseorang yang merasa dirugikan akibat kegiatan melanggar pasal – pasal tersebut, seseorang yang dirugikan dapat langsung mengajukan gugatan untuk meminta ganti rugi dan pelaku berhak mendapatkan hukuman atas perilaku yang merugikan korban tersebut.

Untuk melengkapi teori-teori yang dapat memperkuat artikel dalam poin data privasi, menggunakan beberapa artikel terdahulu yang bisa dicari dengan beberapa kata kunci, seperti: data, privasi data, pasal penjeratan privasi data, UU ITE.

D. Hipotesis Penelitian

Terdapat beberapa kalimat pernyataan hipotesa yang dapat membangun jawaban dan diskusi mengenai hasil artikel. Penganalisaan dari hipotesa yang dituliskan akan dimasukkan kedalam point 4 terkait hasil dan analisis.

H1: Tantangan yang cukup banyak untuk penerapan kabupaten atau kota dalam mengikuti gerakan *Smart-City*.

Hipotesis pertama ini diambil berdasarkan artikel mengenai tantangan yang akan dilalui kabupaten atau kota jika menerapkan gerakan *SmartCity*. Terdapat beberapa tantangan yang dijabarkan seperti IoT dimasa depan akan digunakan lebih banyak dalam keamanan jaringan terutama jika akan menerapakan gerakan *SmartCity*, sehingga pemahaman akan teknologi IoT juga harus diperbanyak dan diperdalam. Selanjutnya harus menentukan solusi keamanan lainnya yang realistis terhadap kemampuan dan anggaran namun tetap mempertimbangkan tindakan pencegahan jika sewaktu-waktu terdapat case yang terjadi [13].

H2: Keamanan dan privasi data teroptimalkan dengan teknologi yang canggih.

Hipotesis kedua ini diambil berdasarkan artikel mengenai tantangan keamanan dan privasi data jika *SmartCity* diterapkan dalam beberapa kabupaten ataupun kota. Jadi, jika selama ini dalam sistem keamanan privasi data menggunakan sistem berbasi FOG maka akan ada tantangan baru dalam sistem keamannya jika menerapkan gerakan *SmartCity* karena jika dilihat dari sistem FOG nya sendiri akan rentan terhadap serangan hacker dibandingkan dengan yang menggunakan sistem berbasis cloud yang berpusat [14]. Selanjutnya, pemerintah harus menyediakan teknologi IoT agar bisa meminimalisasi data yang sudah dikumpulkan, digunakan maupun disimpan, sehingga akan memudahkan dalam pemindahan data [15].

III. METODOLOGI PENELITIAN

Metodologi penelitian akan membahas mengenai bagaimana alur dalam tinjauan literatur untuk memperjelas arah penelitian dalam artikel. Tahapan tinjauan literatur disini menggunakan metode SLR atau systematic literature review, yang mana dalam metode ini akan mencangkup semuanya mulai dari mengidentifikasi jurnal sebelumnya, menilai baik buruknya jurnal sebelumnya yang akan digunakan dalam referensi, dan menginterpretasi temuan-temuan yang ditemukan dari jurnal – jurnal sebelumnya yang menjadi referensi guna menjawab hipotesa yang sudah disusun. Detail alur dalam metodologi penelitian dapat dilihat pada Gambar 5.

TABEL I. MENGIDENTIFIKASI PENELITIAN SEBELUMNYA

Literatur	Pembahasan	Temuan	Kekurangan
Kategori: Fokus terhadap *Smart-City*			
[37]	Menyelidiki studi yang membahas mengenai aspek ketahanan siber dan bagaimana respon DFIR dari CPS pada *Smart-City* berdasarkan literatur review	CPS yang menangani mengenai ketahanan dalam dunia maya dan dukungan untuk DFIR akan menjadi paradigma dan trend di masa yang akan datang pada sistem *Smart-City*.	Kumpulan sumber daya ilmiah yang digunakan dalam penelitian masih terbatas sehingga masih ada batasan dalam kemampuan bereksperimen.
[32]	Sistem *Smart-City* akan membutuhkan jaringan 5G untuk penyediaan layanan internet dalam penggunaan big data	Jaringan syaraf acak 5G yang menggunakan teknologi *blockchain* telah divalidasi mampu meningkatkan konektivitas, ketahanan keamanan siber, dan dapat membuat akses pengguna yang terdesentralisasi.	Hanya menggunakan satu jenis jaringan syaraf dengan teknologi *blockchain* sehingga tidak ada perbandingan hasil jika menggunakan teknologi lain atau menambahkan jaringan syaraf lainnya.
Kategori: Fokus terhadap Keamanan Siber (*Cyber Security*)			
[50]	Bagaimana survey secara komprehensif menangani masalah keamanan dan data privasi dalam sistem *Smart-City*	Membuat taksonomi untuk sistem *Smart-City* berdasarkan arsitektur komponen-komponen, pilar dan aplikasi utamanya.	Sudah diidentifikasi berbagai tantangan utama mendatang namun tidak memberikan penjelasan saran teknologi yang dapat mengatasi tantangan utama tersebut.
Kategori: Fokus terhadap Keamanan Siber dalam penerapan *Smart-City*			
[31]	Gambaran mengenai masalah keamanan yang utama dalam penerapan *Smart-City* dan solusinya dengan berdasarkan tinjauan literatur	Terdapat ancaman yang akan mengintimidasi integrasi infrastruktur *Smart-City* kedepannya seperti: *eavesdropping, theft, DoS, software crashing, hardware failure, etc.*	Penelitian ini dilakukan pada tahun 2017 sehingga jika ditelaah dengan kondisi yang sekarang masih banyak saran teknologi yang kurang mendukung untuk *Smart-City* di masa yang akan datang.
	Faktor yang akan mempengaruhi keamanan data privasi dan informasi data nya dalam sistem *Smart-City*	Tantangan yang akan dihadapi terkait data privasi terbagi menjadi 4 yaitu tantangan terkait warga dalam kabupaten yang akan menjadi *Smart-City,* komunikasi M2M, lalu tantangan dibidang perbankanan dan bisnis pribadi.	
[33]	Melakukan survei dan diskusi dengan menggunakan tinjauan literatur yang berfokus dengan empat komponen utama yang diterapkan dalam sistem *Smart-City*	Dua isu kompleks dan penting adalah data privasi dan keamanan siber untuk penggunaan sistem *Smart-City*.	Kurangnya mekanisme dalam menilai dan memberi peringkat tantangan dan solusi dalam menghadapi sistem *Smart-City*
		Tingkat serangan dan kerentanan akan meningkat dengan mengintegrasikan dan menghubungkan beberapa sistem dalam *Smart-City*.	
		Tanpa teknologi yang canggih semakin banyak data yang dihasilkan terkait lokasi dan aktivitas pada dunia digital maka privasi akan semakin tidak stabil dalam *Smart-City*.	
[38]	Menilai bagaimana langkah dalam keamanan siber dengan fokus terhadap standar teknis dan kerangka peraturan dalam sistem *Smart-City*	Kerangka yang direkomendasikan sudah mencangkup standar teknis, kerangka peraturan dan jaminan untuk memastikan bahwa seluruh keamanan dapat diterapkan dalam semua lapisan pada *Smart-City*.	Penelitian yang dilakukan hanya berdasarkan tinjauan yang terbuka secara umum, tidak melibatkan studi lapangan atau wawancara secara langsung.
[39]	Mengidentifikasi dari berbagai area yang termasuk *Smart-City* yang terpengaruh terhadap tantangan keamanan siber dan mengetahui peringkat tekanan masing-masing area.	Faktor *Smart-security* menjadi faktor paling penting yang akan dipengaruhi oleh kemanan siber dan faktor yang tidak signifikan adalah faktor *Smart-building*	Kerangka yang digunakan masih menggunakan konseptual sederhana sehingga kurang menemukan solusi untuk setiap tantangan kemanan siber dalam sistem *Smart-City*.
Kategori: Fokus terhadap Data Privasi			
[45]	Mensistematisasikan area aplikasi, tipe privasi, mengaktifkan teknologi, dan mencari sumber data untuk serangan	Menciptakan taksonomi yang memungkinkan analisis holistik dari ancaman privasi dan solusi yang memungkinkan	Solusi privasi komprehensif untuk *Smart-City* dijelaskan hanya sesuai teknik tidak dijabarkan secara mendetail dasar penggunaan teknologi tersebut.
	Teknologi untuk peningkatan privasi yang dapat digunakan untuk meninjau keadaaan *Smart-City* di seluruh dunia	Menemukan banyak teknik utilitas yang netral yang menunjukan bahwa *trade-off* digabungkan dengan privasi utulitas hasilnya tidak sebagus yang diperkirakan	
Kategori: Fokus terhadap Data Privasi dalam penerapan *Smart-City*			
[34]	Bagaimana pengelolaan keamanan siber dan data privasi yang dilihat dari berbagai sudut pandang ketahanan digital	Analisa *trade-off* antara potensi biaya insiden dengan dampak pada kinerja proses bisnis dapat menyebabkan beberapa efek buruk	Hanya memberikan hasil analisa menggunakan *trade-off* dengan berbagai kekurangannya namun tidak memberikan saran lebih baik perusahaan menggunakan teknologi apa agar mengurangi resiko, biaya dan manfaat.

Gambar 5 menunjukkan tahapan tahapan yang dilakukan dalam artiker tinnjauan literatur review. Dikarenakan tahapan pertama atau perencanaan sudah di jelaskan secara detail diatas, maka dalam point 3 ini akan langsung membahas pada tahapan pelaksanaan. Untuk tahapan pelaporan yang hasil akhirnya terdapat hasil, kesimpulan, dan saran akan dijelaskan secara detail dalam point 4 dan point 5. Terdapat 20 artikel atau jurnal penelitian sebelumnya yang sudah di pilih sesuai topik, objek, dan permasalahannya. Namun dalam penelitian sebelumnya, banyak yang sudah menggunakan objek dan topik yang sama, namun untuk studi kasus di Indonesia belum ada yang membahas mengenai data privasi dan keamanan siber dalam penerapan *Smart-City* dalam sebuah artikel secara bersamaan. Beberapa artikel

TABEL II. MENGIDENTIFIKASI PENELITIAN SEBELUMNYA LANJUTAN

Literatur	Pembahasan	Temuan	Kekurangan
Kategori: Fokus terhadap Data Privasi dalam penerapan *Smart-City*			
[46]	Bagaimana kerangka kerja yang mampu menangani IoT dan mampu menjaga keamanan data privasi dalam sistem *Smart-City*	Mengusulkan kerangka kerja untuk memastikan keamanan dan melindungi data privasi masyarakat untuk sistem *Smart-City*	Tidak ada penjelasan mengenai bagaimana cara menjaga privasi selama eksekusi proses analitik data privasi.
Kategori: Fokus terhadap Data Privasi dan Keamanan Siber dalam penerapan *Smart-City*			
[35]	Apa saja faktor – faktor yang dapat diterapkan dalam *Smart-City* agar jaringan 5G dapat berhasil dalam hal keamanan dan data privasi	Kebanyakan faktor-faktor penting yang efektif dan kritis untuk mencapai jaringan terbaik yang berhasil terdeteksi menggunakan analisis komponen utama atau PCA. Arsitektur IoT akan menjadi peran yang penting dalam membentuk gelombang dalam *Smart-City* karena akan membangun sistem kontrol akses yang lebih cerdas untuk mengatasi tantangannya.	Kurangnya hasil dan analisa yang mendetail dari setiap analisa yang dilakukan.
[40]	Menyelidiki bagaimana resiko yang ada pada jejaring sosial online yang akan mempengaruhi *Smart-City* Mempelajari apa saja perbedaan antara ancaman privasi dan keamannya yang ditinjau dari komponen sistem *Smart-City*	Model hubungan yang diusulkan dari ancaman privasi data dan keamanan dapat memahami kebutuhan pengguna dan meningkatkan privasi dan keamanan dalam sistem *Smart-City*	Sampel data yang diambil hanya satu area sehingga untuk hasil dari mempelajari dan mengidentifikasi tidak bisa diterapkan jika berada pada daerah lain
[41]	Bagaimana solusi teknis yang tersedia dari sistem *e-government* mengenai keamanan dan privasi data di lingkungan sistem *Smart-City*	Mengusulkan kerangka kerja *e-government* yang aman, terdesentralisasi dan mampu menjaga privasi menggunakan teknologi *blockchain* dan kemajuan AI.	Kurangnya waktu dan research untuk memvalidasi dalam pengklasifikasi dengan kondisi waktu nyata dalam teknologi kemajuan AI dan *blockchain*.
[42]	Bagaimana keamanan siber dan data privasi dilihat dari konsep *Smart-transportation* yang berfokus pada peran mobil pribadi	Keamanan dan privasi data pada *Smart-transportation* bukan hanya masalah teknis, namun juga masalah sosial dan internasional dan masalah multi-budaya.	Tidak ada saran untuk menghadapi tantangan dan masalah mendasar mengenai keamanan dan privasi pada *Smart-transportation*
[43]	Masalah privasi dan keamanan dalam aplikasi pintar yang sudah terintegrasi dengan persyaratan yang sesuai untuk membangun *Smart-City* yang aman dan stabil.	Teknologi keamanan dan perlindungan yang dirasa mampu untuk membantu dalam sistem *Smart-City* seperti *crypthography, ontology, blockchain*, dll.	Tidak dijelaskan metode perlindungan apa yang lebih efektif yang perlu dikembagnkan untuk mengimbangi pertumbuhan *Smart-City* dengan cepat.
[44]	Bagaimana cara mengamankan privasi data yang tersembunyi pada data dalam sistem *Smart-City* yang belum diintegrasikan	Kinerja yang diprediksi oleh penelitian menunjukan hasil yang lebih baik menggunaakan teknik *locality-sensitive hashing* (LSH) dari pendeketan kompetitif lainnya	Fusi data dan model prediksi yang digunakan dalam penelitian masih dalam konteks yang kecil dan sederhana.
[47]	Mengembangkan kerangka kerja interaksi pada *Smart-City*, menganalisa banyak tantangan pada *Smart-City*	Faktor penting yang berkaitan terhadap tata kelola teknis dan keamanan pada sistem *Smart-City* yaitu faktor yang berhubungan dengan integritas operasional dan kepercayaan masyarakat terhadap infrastruktur *Smart-City*.	Fokus penelitian hanya sebatas keamanan dan privasi dapat yang hanya berpusat dampaknya pada masyarakat ketika penerapan *Smart-City* dilakukan.
[48]	Tantangan privasi data dalam penerapan *smat-City* di Indonesia	Indonesia belum menemukan pendekatan regulasi untuk memastikan perlindungan data privasi	Menganalisa hanya dilihat berdasarkan hukum saja, tinjauan literaturnya tidak ada yang berasal dari dunia IT.
[49]	Bagaimana platform IoT dalam mengamankan aspek privasi data dan keamanan GDPR pada sistem *Smart-City*	Dalam beberapa tantangan keamanan pada sistem *Smart-City*, arsitektur IoT Snap4*City* terbukti telah memnuhi semua persyaratan yang diajukan.	Hanya menguji dan melihat dari teknologi Snap4*City* namun mampu memberikan kesimpulan bahwa Snap4*City* telah diidentifikasi sebagai solusi pemenang keamanan dalam *Smart-City*.

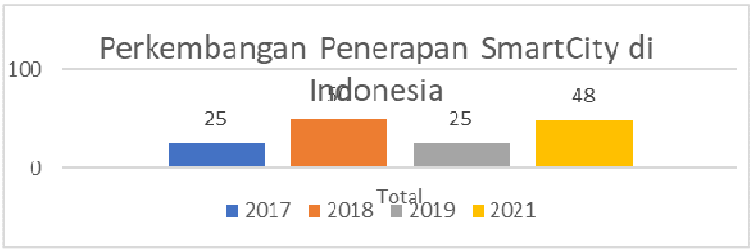
lebih fokus terhadap satu objek seperti satu artikel hanya membahas mengenai bagaimana data privasi jika sebuah kota diterapkan sistem *Smart-City* seperti pada artikel [45] dan juga satu artikel hanya membahas mengenai bagaimana tingkat keamanan siber jika sebuah kabupaten maupun kota menerapkan *Smart-City* seperti pada artikel [50]. Untuk lebih lengkap mengenai penjelasan dari artikel yang relevan sebelumnya dapat dilihat pada Tabel I dan Tabel II.

Tabel I dan Tabel II menunjukan beragam variasi pembahasan yang terdapat dalam penelitian sebelumnya, begitupula dengan temuan – temuan yang dapat dianalisa bagaimana jika akan diterapkan dalam beberapa tahun kedepan. Terdapat juga berbagai kekurangan dari masing-masing jurnal yang bisa dijadikan penelitian terbaru bagaimana cara penanganan kekurangan agar menjadikan penelitian baru yang lengkap dengan penjelasannya juga.

IV. HASIL DAN ANALISIS

Hasil dan analisis disini akan terdapat beberapa point, point pertama ingin melihat dan menjelaskan mengenai perkembangan setiap tahunnya dalam pengupayaan pemerintah untuk menggencarkan kegiatan *Smart-City* di Indonesia seperti yang ada pada Gambar 6. Data yang diambil disini sudah berdasarkan research dari berita ataupun jurnal-jurnal sebelumnya yang pernah membahas hal yang serupa.

Pada Gambar 6, untuk tahun 2022 pemerintah sudah menargetkan 50 kabupaten atau kota pilihan yang



Gambar 6. Perkembangan *Smart-City* di Indonesia [16]

selanjutnya akan menerapkan dan mengikuti gerakan *Smart-City* [16]. Setelah melihat dari perkembangan kabupaten atau kota yang sudah menerapkan *Smart-City* di Indonesia.

Point selanjutnya membahas mengenai bagaimana hasil dari pernyataan hipotesa yang sudah dibuat pada point 2 dan melihat hasil dari pengidentifikasian pada Tabel 1 dan Tabel 2. Hipotesa pertama yang membahas mengenai tantangan yang cukup banyak jika kabupaten ataupun kota akan menerapkan sistem *Smart-City*. Jika dilihat dari hasil pengidentifikasian jurnal sebelumnya tantangan yang terbanyak yang akan ditemui oleh kabupaten ataupun kota ketika ingin menerapkan sistem *Smart-City* yaitu mengenai data privasi kabupaten atau kota maupun data privasi oleh masyarakat yang sebelumnya tidak menggunakan bantuan teknologi secara menyeluruh, lalu tantangan selanjutnya yaitu memberi pemahaman yang lebih terhadapa masyarakat yang kabupaten ataupun kotanya akan menggunakan sistem *Smart-City* , karena ini juga merupakan salah satu komponen atau infrastruktur jika suatu kabupaten atau kota ingin menerapkan sistem *Smart-City* yaitu infrastruktur *Smart-society* atau masyarakat yang cerdas. Setelah menganalisa dan melihat dari berbagai sudut pandang yang ada pada beberapa penelitian sebelumnya, jika suatu kabupaten ataupun kota akan menerapkan sistem *Smart-City* maka akan banyak tantangan yang beresiko.

Hipotesa selanjutnya yaitu mengenai keamanan dan data privasi dapat teroptimalkan jika menggunakan teknologi yang canggih. Jika dianalisa dari hasil pengidentifikasian jurnal sebelumnya pada Tabel 1 dan Tabel 2 maka hasil dari hipotesa kedua ini adalah benar, semakin canggih teknologi yang digunakan maka data privasi dan keamanan sibernya juga akan terlindungi secara optimal. Namun, sesuai jurnal sebelumnya jika sistem *Smart-City* di Indonesia masih belum terlalu maksimal karena teknologi yang digunakan masih tergolong baru bahkan ahli-ahli yang mengerti dan memahami teknologi tersebut masih sangat sedikit. Tetapi, jika ingin sistem *Smart-City* tetap diterapkan pada Indonesia, dapat melihat beberapa rekomendasi teknologi beserta penjelasannya dari berbagai dunia yang sudah berhasil menerapkan dan menjalankan sistem *Smart-City* ini. Tabel 3 menjelaskan beberapa perbandingan infrastruktur dari yang sudah diterapkan di negara lain dan dapat diterapkan di Indonesia agar meningkatkan sistem keamanan dan data privasinya, beserta contoh penggunaan teknologi yang digunakan sesuai jurnal – jurnal referensi sebelumnya.

Tabel 3 menjelaskan berbagai kategori dengan teknologi yang dapat digunakan jika di Indonesia ingin menggunakan sistem keamanan dan perlindungan data privasi yang canggih. Jika dalam hal tantangan keamanan siber dalam sistem *Smart-City* dapat menerapkan teknologi dari kategori blockchain, ontology dan cyber-security. Sedangkan, jika dalam hal perlindungan data privasi kabupaten atau kota maupun masyarakat dapat menggunakan teknologi dari kategori DM dan ML dan ontology yang point terakhir. Agar masyarakat yang kabupaten ataupun kotanya akan menjadi *Smart-City* dapat percaya dan yakin bahwa jika dengan penerapan *Smart-City* pada kotanya maka data data privasi akan selalu aman dan seluruh kegiatan yang dilakukan dalam dunia digital juga akan aman, kalaupun ada yang tidak aman maka berikan kepercayaan bahwa terdapat hukum yang jelas melindungi privasi dan keamanan masyarakat.

Dilihat dari Tabel 3, teknologi yang kemungkinan ketika

TABEL III. TEKNOLOGI KEMANAN SIBER DAN DATA PRIVASI PADA *SMART-CITY*

Kategori	Referensi	Teknologi Yang Disarankan
Blockchain	[17], [28]	Menggunakan jaringan jenis topologi dengan jenis framework desentralisasi *blockchain* contoh casenya menggunakan aplikasi transportasi cerdas atau *Smart transportation*
	[18]	Mendistribusikan beberapa teknologi yang dilihat dari teknik *blockchain* dan sistem FOG dengan contoh casenya menggunakan teknologi IoT arsitektur
Ontology	[19]	Mengontrol seluruh privasi pribadi dan konten konten dalam data privasi contoh penggunaan aplikasinya dapat menggunakan sistem *mobile computing*
	[20]	Mengontrol segala situasi yang berdasarkan penalaran dengan menggunakan basis ontologi semantik dan contoh casenya dapat menggunakan teknologi IoT arsitektur
	[21], [30]	Menggunakan teknologi ICADS untuk membantu pengintegrasian *Smart ontology* dalam sisi keamanan data dan keamana siber *Smart-City*.
DM and ML	[22], [27]	Menggunakan jenis atau sistem pembelajaran fitur yang mendalam contoh case penerapannya dapat dilakukan pada jaringan Wi-Fi
	[23]	Menggunakan sistem autentikasi *Smartphone* berbasis dari SVM dan dapat menggunakan model regresi linear Bayyes seperti yang sudah diterapkan sebelumnya
	[24]	Menggunakan methode HSCCA untuk melindungi dari penyerangan terhadap keamanan siber dan data privasi dengan level HSCCA yang tinggi untuk bisa di lakukan setting dalam *Smart-City*
	[25]	Untuk pengamanan data dalam cyber security dapat menggunaakan data-driven agar dapat mengintegrasikan beberapa teknologi yang memiliki teknik tinggi agar bisa saling relevan
	[26], [29]	Menggunakana sebuah autentikasi yang berbasis biometrik dan juga memasang protokol – protokol negosiasi menggunakan kuncinya masing – masing, contoh case dalam penerapan ini dapat dilakukan pada perangakat penyimpanan dalam setiap *Smart-City*

diterapkan dalam sistem *Smart-City* di Indonesia mampu menyeimbangi *Smart-City* di negara lain, di masing-masing kategorinya terdapat 1 teknologi yang setelah diuji dalam penelitian sebelumnya sudah sukses diterapkan. Dalam kategori blockchain teknologi yang disarankan dan sukses berhasil diterapkan yaitu framework blockchain yang diterapkan pada *Smart*-transportation, lalu untuk kategori ontology dapat menggunakan teknologi ICADS yang dapat membantu pengintegrasian *Smart*-ontology dalam *Smart-City*, kategori ketiga DM dan ML dapat menggunakna teknologi sistem keamanan yang canggih yang diterapkan dalam jaringan WiFi, dan kategori terakhir atau kategori cyber security terdapat satu teknologi yang sudah diterapkan dalam beberapa negara berhasil yakni menggunakan teknologi yang berbasis biometrik dengan protokol – protokolnya yang dapat diterapkan dalam perangkat penyimpanan data dalam sistem *Smart-City*.

V. DISKUSI

Tabel 1 dan Tabel 2 menunjukan berbagai identifikasi mengenai temuan, tantangan, bahkan masalah yang dihadapi dalam perlindungan data privasi dan keamanan siber yang diterapkan dalam sistem *Smart-City* di beberapa dunia berdasarkan tinjauan pustaka atau referensi yang sudah dipilih dan disaring untuk dijadikan dasar dari artikel ini. Jika penerapan *Smart-City* dalam negara lain tantangan dan masalah utama dalam penerapannya terdapat pada bagaimana sistem keamanan data dari sistem biasa menjadi sistem *Smart-City*. Sedangkan, apakah sistem *Smart-City* jika diterapkan di Indonesia hanya masalah tersebut yang menjadi masalah utama. Dikarenakan, berdasarkan jurnal referensi, beberapa kabupaten maupun kota yang sudah menerapkan sistem *Smart-City* tantangan dan masalah penting selain keamanan data ataua bagaimana meyakinkan masyarakat agar dapat menerima seluruh aktivitas yang akan dilakukan jika kabupaten maupun kotanya akan menjadi *Smart-City*, karena masyarakat juga merupakan salah satu dari enam (6) komponen atau infrastruktur yang wajib diterapkan kabupaten ataupun kota jika ingin menerapkan sistem *Smart-City*. Selain itu, usaha pemerintah juga akan susah jika penerapan *Smart-City* di Indonesia tidak diseimbangin dengan pengetahuan akan bagaimana data privasi dan keamanan seluruh kegiatan dari dunia maya dapat terjamin keamanannya. Dan dikarenakan Indonesia merupakan negara yang berpedoman akan hukum, maka juga perlu dipertimbangkan apakah hukum di Indonesia sudah cukup mewadahi jika sewaktu-waktu terdapat banyak kasus kejahatan yang dilakukan dalam aktivitas online pada *Smart-City*. Karena, yang dilihat berdasarkan referensi atau tinjauan pustaka sebelumnya, hukum di Indonesia masih kurang untuk mampu melindungi data privasi masyarakatnya dan dari penelitian sebelumnya juga menuliskan bahwa teknologi yang berada di Indonesia untuk diterapkan dalam sistem *Smart-City* masih belum secanggih yang diterapkan pada negara lain, sehingga seharusnya ini menjadi suatu pertimbangan pemerintah di masa yang akan datang, agar kabupaten maupun kota yang sudah maupun belum menerapkan sistem *Smart-City* lebih percaya dan yakin akan sistem baru yang akan diterapkan pada kabupaten maupun kotanya.

VI. KESIMPULAN DAN SARAN

Kebijakan pemerintah dalam menerapkan gerakan *Smart-City* di Indonesia agar dapat menyesuaikan dengan perkembangan teknologi yang semakin canggih di setiap tahunnya. Terutama dalam penerapan gerakan tersebut dari satu kabupaten ke kabupaten lain yang sekarang sudah mencapai 191 kabupaten atau kota di Indonesia yang sudah menerapkan menggunakan *Smart-City*. Walaupun sudah terlihat hasil penerapannya dan sudah berhasil menjalankan menggunakan teknologi baru, program kerja setelah penerapan *Smart-City* ternyata masih ada beberapa hal atau infrastruktur yang perlu diterapkan agar sekaligus dapat melindungi keamanan siber dan data privasi baik data dari pemerintahan maupun data pribadi milik seorangan. Pada Tabel 3 sudah dijelaskan beberapa kemungkinan teknologi yang dapat diterapkan dan diambil untuk penyesuaian *Smart-City* agar gerakan ini bisa seimbang dengan *Smart-City* yang diterapkan dalam negara – negara lain. Terutama harus diperkuat dari sisi keamanan karena ini menyangkut sebuah kabupaten ataupun kota sehingga keamanan yang menjadi poin penting agar tidak diretas, agar tidak terjadi kebocoran data, agar dapat tidak sembarang orang menggunakan data orang lain dan agar pemerintah dapat melindungi data privasi milik warga dan kabupaten setempat. Dari beberapa jurnal yang sudah dijabarkan, saran utama dalam pengefisienan, penguatan keamanan dll dapat menggunakan teknologi IoT arsitektur yang mana di beberapa negara sudah diterapkan teknologi tersebut dan hasilnya keamanan dan jaringan yang saling terhubung jadi lebih kuat dan lebih aman. Selain teknologi IoT arsitektur terdapat satu teknologi yang dapat diterapkan selanjutnya dalam sistem *Smart-City* di Indonesia, yaitu teknologi blockchain, jika dilihat pada negara-negara yang sudah menerapkan sistem *Smart-City* dilihat dari jurnal – jurnal referensi, teknologi blockchain mampu menangani masalah dan tantangan kompleks yang terjadi dan terbentuk akibat perubahan sistem biasa menjadi sistem *Smart-City* dalam suatu kabupaten, kota maupun negara. Namun, adapula kekurangan dalam artikel ini dikarenakan objek yang diambil hanya dua dari sekian banyak objek yang ada di dalam *Smart-City* lalu untuk menganalisa dan mengumpulkan data – datanya masih kurang banyak sehingga solusi teknologi yang ditawarkan juga masih sedikit. Dua objek ini memang objek terpenting jika ingin dilakukan analisa mengenai penerapan *Smart-City* di Indonesia namun masih banyak objek objek pendukung yang mampu memperkuat dan menyempurnakan gerakan *Smart-City* di Indonesia. Dan juga karena keterbatasan waktu dalam pembuatan artikel atau jurnal dalam penelitian, sehingga data – data yang diambil untuk referensi hanya berasal dari jurnal sebelumnya yang terbuka oleh umum, belum ada data yang berasal dari masyarakat yang kotanya sudah menerapkan sistem *Smart-City* atau bahkan beberapa orang dari pemerintah Indonesia yang sudah berhasil menerapkan sistem *Smart-City* di 100 lebih kabupaten ataupun kota yang berada di Indonesia. Sehingga kedepannya, jika akan dilakukan penelitian atau pembuatan jurnal yang serupa data yang digunakan bukan hanya berasal dari jurnal – jurnal sebelumnya, namun dapat juga mengambil survey masyarakat yang kabupaten ataupu kotanya sudah menerapkan sistem *Smart-City*, dan juga dapat mengambil data menggunakan wawancara secara langsung kepada pemerintah ataupun orang yang terlibat dalam penerapan sistem *Smart-City* di Indonesia.

DAFTAR PUSTAKA

[1] E. Devega, "Langkah Menuju '100 *Smart City*'," Sorotan Media. 2017. Retrieved from https://kominfo.go.id/content/detail/11656/langkah-menuju-100-*Smart-City*/0/sorotan_media

[2] A. Panatagama, "Perkembangan dan Masa Depan *Smart City* Indonesia," Terralogiq. 2021. Retrieved from https://terralogiq.com/perkembangan-dan-masa-depan-*Smart*-*City*-indonesia/

[3] M. Alamer & M. A. Almaiah, "Cybersecurity in *Smart City*: A Systematic Mapping Study," International Conference on Information Technology - ICIT 2021. January 2021, pp. 719-724. https://doi.org/10.1109/ICIT52682.2021.9491123

[4] H. Habibzadeh, B. Nussbaum, F. Anjomshoa, B. Kantarci & T. Soyata, "A survey on cybersecurity, data privacy, and policy issues in cyber-physical system deployments in *Smart* cities," Sustainable Cities and Society. Vol. 50, October 2019, 101660. https://doi.org/10.1016/j.scs.2019.101660

[5] Adminpu, "*Smart City*: All We Need To Know," *Smart City*, definisi dan pengertian. Retrieved from https://dpu.kulonprogokab.go.id/detil/68/*Smart*-*City*-definisi-dan-pengertian.

[6] T. Bjørner, "The advantages of and barriers to being *Smart* in a *Smart City*: The perceptions of project managers within a *Smart City* cluster project in Greater Copenhagen," Cities. Vol. 114, 2021, 103187.

[7] A. Caragliu, C. Del Bo & P. Nijkamp, "*Smart* Cities in Europe," Journal of Urban Technology. Vol. 18, Issue 2, 2011, pp. 65-82.

[8] L. Rizkinaswara, "Mengenal Lebih Dekat Konsep *Smart City* dalam Pembangunan Kota," Ditjen Aplikasi Informatika. 2020. Retrieved from https://aptika.kominfo.go.id/2020/10/mengenal-lebih-dekat-konsep-*Smart*-*City*-dalam-pembangunan-kota/

[9] F. A. Firman, "Kebijakan Pertahanan Cyber Estonia Dalam Merespon Tindakan Cyber Sabotage Oleh Rusia Kepada Estonia," Diploma thesis, Universitas Komputer Indonesia. 2018.

[10] B. Gunes, G. Kayisoglu & P. Bolat, "Cyber security risk assessment for seaports: A case study of a container port," Computers & Security, Vol. 103, pp. 102196.

[11] S. Dewi, Cyber law : perlindungan privasi atas informasi pribadi dalam ecommerce menurut hukum internasional, Monograf, Bandung, Widya Padjdjaran, 2009.

[12] A. Dony, Kriptografi Keamanan Data dan Komunikasi. Graha Ilmu, Yogyakarta, 2006.

[13] S. Yu, G. Gu, A. Barnawi, S. Guo & I. Stojmenovic, "Propagasi malware dalam jaringan skala besar," IEEE Transactions on Knowledge and Data Engineering, Vol. 27, No. 1, pp. 170–179, 2015.

[14] D. Puthal, S. Nepal, R. Ranjan & J. Chen, "Ancaman terhadap jaringan cloud dan pusat data tepi di Internet of Things," IEEE Cloud Computing, Vol. 3, No. 3, pp. 64–71, 2016.

[15] C. Perera, C. Mccormick, A. K. Bandara, B. A. Price & B. Nuseibeh, "Privacy-by-Design Framework for Assessing Internet of Things Applications and Platforms," 6th International Conference on the Internet of Things (IoT 2016), 2016.

[16] Z. D. Ulhaq, "Siap Bangun *Smart City* 2022, Kominfo Dorong Kolaborasi dengan 50 Kepala Daerah," 2022. Retrieved from https://www.pikiran-rakyat.com/nasional/pr-014318701/siap-bangun-*Smart*-*City*-2022-kominfo-dorong-kolaborasi-dengan-50-kepala-daerah

[17] A. Lei, H. Cruickshank, Y. Cao, P. Asuquo, C. P. A. Ogah & Z. Sun, "Blockchain-Based Dynamic Key Management for Heterogeneous Intelligent Transportation Systems," IEEE Internet of Things Journal. Vol. 4, pp. 1832 - 1843, 2017.

[18] P. K. Sharma, M. Y. Chen & J. H. Park, "A Software Defined Fog Node Based Distributed Blockchain Cloud Architecture for IoT," IEEE Access Journal, Vol. 6, pp. 115-124, 2018.

[19] K. Seung-Hyun, K. In-Young & K. Soo-Hyung, "Quality of Private Information (QoPI) model for effective representation and prediction of privacy controls in mobile computing," Computers and Security. Vol. 66, Issue May 2017, pp 1–19. https://doi.org/10.1016/j.cose.2017.01.002

[20] G. Xu, Y. Cao, Y. Ren, X. Li & Z. Feng, "Network Security Situation Awareness Based on Semantic Ontology and User-Defined Rules for Internet of Things," IEEE Access, vol. 5, pp. 21046-21056, 2017, doi: 10.1109/ACCESS.2017.2734681.

[21] R. Khatoun & S. Zeadally, "Cybersecurity and Privacy Solutions in *Smart* Cities," IEEE Communications Magazine. Vol. 55, pp. 51-59, 2017.

[22] C. T. Do, N. H. Tran, C. Hong, C. A. Kamhoua, K. A. Kwiat, E. Blasch, S. Ren, N. Pissinou & S. S. Iyengar, "Game theory for cyber security and privacy," ACM Computing Surveys. Vol. 50, Issue No. 2, pp. 30-37, 2017.

[23] A. A. A. Abass, L. Xiao, N. B. Mandayam & Z. Gajic, "Evolutionary Game Theoretic Analysis of Advanced Persistent Threats Against Cloud Storage," IEEE ACCESS, Vol. 5, pp. 8482-8491, 2017.

[24] D. Chen, P. Wawrzynski & L. Zhihan, "Cyber security in *Smart* cities: A review of deep learning-based applications and case studies," Sustainable Cities and Society, pp. 102655, 2020.

[25] T. Qamar & N. Z. Bawany, "A Cyber Security Ontology for *Smart City*," International Journal on Information Technologies & Security, vol. 12, no. 3, 2020.

[26] S. Shamshirband, A. Patel, NB Anuar, MLM Kiah, dan A. Abraham. 2014. "Pendekatan teori permainan kooperatif menggunakan fuzzy Q-learning untuk mendeteksi dan mencegah intrusi dalam jaringan sensor nirkabel,"Ind. aplikasi Arti. Intel., vol. 32, hlm. 228–241.

[27] H. Alshambri, M. A. Al Zain, B. Soh, M. Masud & J. Al-Amri, "Cybersecurity Attacks On Wireless Sensor Networks In *Smart* Cities: An Exposition", International Journal of Scientific & Technology Research. Vol. 8, Issue 01, January 2020.

[28] N. Gupta, V. Gupta, G. Kumar, V. Gupta & D.K. Gupta, "Comparative Evaluation of Efficacy of Interscalene Block vs. Interscalene Block and Superficial Cervical Plexus Block for Fixation of Clavicular Fractures," International Journal of Contemporary Medical Research. Vol. 6, No. 3, pp. 11-13. https://doi.org/10.21276/ijcmr.2019.6.3.22

[29] H. Habibzadeh, B. H. Nussbaum, F. Anjomshoa, B. Kantarci & T. Soyata, "A survey on cybersecurity, data privacy, and policy issues in cyber-physical system deployments in *Smart* cities," Sustainable Cities and Society. Vol. 50, October 2019, 101660.

[30] Z. Szabo, "The Effects of Globalization and Cyber Security on *Smart* Cities," Interdisciplinary Description of Complex Systems. Vol. 17, No. 3, 2019, pp. 503-510.

[31] A. Aldairi & L. Tawalbeh, "Cyber Security Attacks on *Smart* Cities and Associated Mobile Technologies," Procedia Computer Science. 109C, 2017, pp. 1086-1091.

[32] S. Smys, H. Wang & A. Basar, "5G Network Simulation in *Smart* Cities using Neural Network Algorithm," Journal of Artificial Intelligence and Capsule Networks. Vol. 3, No. 1, March 2021, pp. 43-52.

[33] C. Ma, "*Smart City* and cyber-security; technologies used, leading challenges and future recommendations," Energy Reports. Vol. 67, November 2021, pp. 7999-8012.

[34] D. Vanderbist, "Digital Resilience: Managing Cyber-Security and Data Privacy," EMBA Vlerick Business School. April 2020.

[35] S. Chatterjee, A. K. Kar & M. P. Gupta, "Critical Success Factors to Establish 5G Network in *Smart* Cities: Inputs for Security and Privacy," In book: *Smart* Cities and *Smart* Spaces (pp. 386-410), January 2019.

[36] M. A. Hasbini & M. Tom-Petersen, "The *Smart* Cities Internet of Access Control, opportunities and cybersecurity challenges," Information Security for *Smart* cities Project. September 2017.

[37] G. Ahmadi-Assalemi, H. Al-Khateeb, G. Epiphaniou & C. Maple, "Cyber Resilience and Incident Response in *Smart* Cities: A Systematic Literature Review," *Smart* Cities 2020, Vol. 3, No. 3, pp. 894-927.

[38] M. Vitunskaite, Y. He, T. Brandstetter & H. Janicke, "*Smart* cities and cyber security: Are we there yet?A comparative study on the role of standards, third party risk management and security ownership," Computers & Security. Vol. 83, June 2019, pp. 313-331.

[39] M. R. Belgaum, Z. Alansari, R. Jain & J. Alshaer, "A Framework for Evaluation of Cyber Security Challenges in *Smart* Cities," *Smart* Cities Symposium in Collaboration with IET-EMEA (SCS'18), 2018, pp. 17-22.

[40] V. Moustaka, Z. Theodosiou, A. Vakali & A. Kounoudes, "*Smart* Cities at Risk!: Privacy and Security Borderlines from Social Networking in Cities," Companion Proceedings of the The Web Conference 2018, pp. 905-910.

[41] L. Yang, N. Elisa & N. Eliot, "Chapter 7 - Privacy and Security Aspects of E-Government in *Smart* Cities," *Smart* Cities Cybersecurity and Privacy, 2019, pp. 89-102.

[42] H. Olufowobi & G. Bloom, "Chapter 16 - Connected Cars: Automotive Cybersecurity and Privacy for *Smart* Cities," *Smart* Cities Cybersecurity and Privacy, 2019, pp. 227-240.

[43] L. Cui, G. Xie, Y. Qu, L. Gao and Y. Yang, "Security and Privacy in *Smart* Cities: Challenges and Opportunities," in IEEE Access, vol. 6, pp. 46134-46145, 2018, doi: 10.1109/ACCESS.2018.2853985.

[44] L. Qi, C. Hu, X. Zhang, M. R. Khosravi, S. Sharma, S. Pang & T. Wang, "Privacy-Aware Data Fusion and Prediction With Spatial-Temporal Context for *Smart City* Industrial Environment," in IEEE Transactions on Industrial Informatics, vol. 17, no. 6, pp. 4159-4167, June 2021, doi: 10.1109/TII.2020.3012157.

[45] D. Eckhoff & I. Wagner, "Privacy in the *Smart City* –Applications, Technologies, Challenges and Solutions," IEEE Communications Surveys & Tutorials. Vol. 20, 2018, pp. 489-516.

[46] M. Witti & D. Konstantas, "A Secure and Privacy-preserving Internet of Things Framework for *Smart City*," Proceedings of the 6th International Conference on Information Technology: IoT and *Smart City*, pp. 145-150, December 2018.

[47] E. Ismagilova, L. Hughes, N. P. Rana & Y. K. Dwivedi, "Security, Privacy and Risks Within *Smart* Cities: Literature Review and Development of a *Smart City* Interaction Framework," Information Systems Frontiers Vol. 24, pp. 393–414, 2022.

[48] S. Dewi Rosadi, Suhardi and S. A. Kristyan, "Privacy challenges in the application of *Smart City* in Indonesia," 2017 International Conference on Information Technology Systems and Innovation (ICITSI), 2017, pp. 405-409, doi: 10.1109/ICITSI.2017.8267978.

[49] C. Badii, P. Bellini, A. Difino and P. Nesi, "*Smart City* IoT Platform Respecting GDPR Privacy and Security Aspects," in IEEE Access, vol. 8, pp. 23601-23623, 2020, doi: 10.1109/ACCESS.2020.2968741.

[50] M. Sookhak, H. Tang, Y. He and F. R. Yu, "Security and Privacy of *Smart* Cities: A Survey, Research Issues and Challenges," in IEEE Communications Surveys & Tutorials, vol. 21, no. 2, pp. 1718-1743, Secondquarter 2019, doi: 10.1109/COMST.2018.2867288.