JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER

p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 4 No 3 February 2026
Hal: 2076-2086
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v4i3.802

Analisis Keamanan dan Kebijakan Privasi dalam Penggunaan Teknologi *Internet of Things* (IoT) untuk *Smart Cities*

Andri Armaginda Siregar[1], Marulak Lasron Siahaan[2], Damri Mulia Hutabalian[3], Jalaluddin Nasution[4], Mhd. Agung Irnanda[5], Naufal Dhiya Putra Dalimunthe[6]

[1,2,3,4,5,6,] Fakultas Teknik & Ilmu Komputer, Universitas Potensi Utama, Kota Medan, Indonesia
Email: [1]andriarmagindasiregar@gmail.com, [2]marulaksiahaan02@gmail.com, [3]damrinainggolan23@gmail.com, [4]jalaluddin.nasution@uinsu.ac.id, [5]agungirnanda16@gmail.com, [6]naufaldhiyaputradalimunthe@gmail.com
(* Email Corresponding Author: andriarmagindasiregar@gmail.com)
Received: January 17, 2026 | Revision: January 22, 2026 | Accepted: January 23, 2026

Abstrak

Perkembangan teknologi *Internet of Things* (IoT) telah menjadi komponen fundamental dalam implementasi *smart cities* melalui pemanfaatan sistem berbasis data untuk meningkatkan efisiensi, kualitas layanan publik, dan pengelolaan infrastruktur perkotaan. Namun, adopsi IoT dalam skala kota juga menghadirkan tantangan signifikan terkait keamanan sistem dan perlindungan privasi data warga. Sistem IoT pada *smart cities* menghasilkan data dalam volume besar, bersifat *real-time*, terdistribusi, dan sering kali mengandung informasi sensitif, sehingga rentan terhadap ancaman keamanan siber dan penyalahgunaan data. Penelitian ini bertujuan untuk menganalisis secara komprehensif aspek keamanan dan kebijakan privasi dalam penggunaan teknologi IoT pada *smart cities* melalui pendekatan terintegrasi. Metode yang digunakan adalah *Systematic Literature Review* (SLR) dengan pendekatan kualitatif deskriptif terhadap 25 publikasi ilmiah terpilih pada periode 2022-2025, yang terdiri dari artikel jurnal, prosiding konferensi, dan dokumen kebijakan yang relevan. Hasil penelitian menunjukkan bahwa ancaman keamanan dan risiko privasi muncul pada seluruh lapisan arsitektur IoT, mulai dari perangkat, jaringan, pengolahan data, hingga aplikasi dan tata kelola. Selain itu, kebijakan privasi yang ada umumnya masih bersifat normatif dan belum sepenuhnya terintegrasi dengan praktik teknis IoT di lapangan. Temuan ini menegaskan bahwa keberhasilan implementasi *smart cities* tidak hanya ditentukan oleh solusi teknis keamanan, tetapi juga oleh efektivitas kebijakan privasi dan tata kelola data yang transparan. Penelitian ini berkontribusi dengan menyajikan kerangka analisis integratif yang menghubungkan keamanan IoT, kebijakan privasi, dan kepercayaan publik sebagai fondasi pengembangan *smart cities* yang berkelanjutan.

Kata Kunci: *Internet of Things, Smart Cities*, Keamanan IoT, Kebijakan Privasi, Tata Kelola Data

Abstract

The rapid development of the Internet of Things (IoT) has become a fundamental component in smart city implementation by enabling data-driven systems to enhance the efficiency of public services and urban infrastructure management. However, large-scale IoT adoption in urban environments also introduces significant challenges related to system security and the protection of citizens' data privacy. IoT-based smart city systems generate massive volumes of real-time, distributed, and often sensitive data, making them highly vulnerable to cyber threats and data misuse. This study aims to comprehensively analyze IoT security and privacy policies in smart cities using an integrated perspective. A qualitative descriptive Systematic Literature Review (SLR) was conducted based on 25 selected publications published between 2022 and 2025, including journal articles, conference proceedings, and policy documents. The findings reveal that security threats and privacy risks exist across all layers of IoT architecture, including device, network, data processing, application, and governance layers. Moreover, existing privacy policies are generally normative in nature and insufficiently aligned with technical IoT implementations. These results highlight that the success of smart city initiatives depends not only on technical security solutions but also on effective privacy policies and transparent data governance. This study contributes by proposing an integrative analytical framework that connects IoT security, privacy policies, and public trust as key pillars for sustainable smart city development.

Keywords*: Internet of Things, Smart Cities, IoT Security, Privacy Policy, Data Governance*

1. PENDAHULUAN

Perkembangan teknologi *Internet of Things* (IoT) telah menjadi elemen kunci dalam transformasi perkotaan menuju konsep *smart cities*. IoT memungkinkan integrasi berbagai perangkat fisik, sensor, dan sistem digital yang saling terhubung untuk mengumpulkan, memproses, dan menganalisis data secara *real-time*, sehingga mendukung pengelolaan kota yang lebih efisien, adaptif, dan berkelanjutan [1]. Dalam implementasinya, IoT dimanfaatkan secara luas pada berbagai sektor strategis perkotaan, seperti transportasi cerdas, manajemen energi, layanan kesehatan, pemerintahan digital, pengelolaan lingkungan, dan infrastruktur publik, dengan tujuan meningkatkan kualitas layanan, efisiensi operasional, serta kualitas hidup masyarakat [2], [3]. Di balik manfaat tersebut, adopsi IoT dalam skala kota juga menghadirkan tantangan serius, khususnya terkait keamanan sistem dan perlindungan privasi data warga. Sistem IoT pada *smart cities* secara inheren menghasilkan data dalam volume besar, bersifat kontinu, *real-time*, dan sering kali mengandung informasi sensitif, seperti data lokasi, pola mobilitas, aktivitas harian, serta informasi kesehatan dan sosial warga [4]. Karakteristik IoT yang heterogen, terdistribusi, dan terhubung melalui jaringan terbuka menjadikannya rentan terhadap berbagai ancaman keamanan siber, termasuk kebocoran data, akses tidak sah, serangan *man-in-the-middle*, serta penyalahgunaan data oleh pihak yang tidak berwenang [5], [6], [16], [21], [24], [25]. Sejumlah penelitian

JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 4 No 3 February 2026
Hal: 2076-2086
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v4i3.802

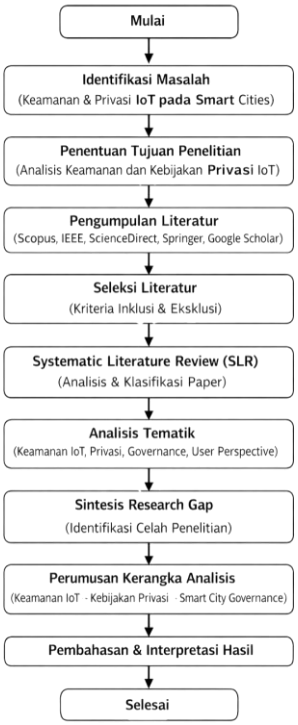
terdahulu telah menyoroti pentingnya keamanan IoT sebagai fondasi utama dalam pengembangan *smart cities*. Berbagai pendekatan teknis telah diusulkan, seperti penerapan mekanisme enkripsi, autentikasi, access control, serta pemanfaatan teknologi pendukung seperti *blockchain, artificial intelligence*, jaringan 5G, dan *digital twin* untuk meningkatkan keandalan dan keamanan sistem IoT [6], [8], [14], [16], [17], [21], [22], [23]. Namun, sebagian besar penelitian tersebut masih berfokus pada aspek teknis dan arsitektur sistem, sementara dimensi kebijakan privasi dan tata kelola data sering kali diperlakukan sebagai isu sekunder dan belum dianalisis secara terintegrasi. Penelitian berbasis *systematic literature review* dan *bibliometric analysis* menunjukkan bahwa riset *smart cities* dan IoT masih cenderung terfragmentasi dan didominasi oleh perspektif teknologi [9], [10]. Aspek kebijakan privasi, regulasi, dan tata kelola data belum memperoleh perhatian yang seimbang, padahal faktor-faktor tersebut memiliki peran penting dalam membangun kepercayaan publik terhadap layanan *smart city* [9], [13], [18], [19], [20]. Selain itu, studi yang mengadopsi perspektif pengguna menunjukkan adanya kesenjangan antara tingkat kekhawatiran masyarakat terhadap privasi data dan rendahnya pemahaman terhadap kebijakan privasi yang berlaku [11], [12]. Kondisi ini mengindikasikan perlunya pendekatan yang lebih holistik dalam menganalisis keamanan dan privasi IoT pada *smart cities*.

Berdasarkan kesenjangan penelitian tersebut, penelitian ini bertujuan untuk menganalisis keamanan dan kebijakan privasi dalam penggunaan teknologi IoT pada *smart cities* secara terintegrasi melalui pendekatan *Systematic Literature Review*. Penelitian ini menganalisis 25 publikasi ilmiah periode 2022-2025 untuk memetakan ancaman keamanan, risiko privasi, serta mengevaluasi kesesuaian antara kebijakan privasi dan praktik teknis IoT. Kontribusi utama penelitian ini adalah penyusunan kerangka analisis integratif yang menghubungkan keamanan IoT, kebijakan privasi, dan tata kelola data sebagai fondasi dalam membangun kepercayaan publik dan mendukung pengembangan *smart cities* yang berkelanjutan.

2. METODOLOGI PENELITIAN

2.1 Desain dan Pendekatan Penelitian

Penelitian ini menggunakan desain penelitian kualitatif deskriptif dengan pendekatan *Systematic Literature Review* (SLR) yang dipadukan dengan analisis konseptual keamanan dan kebijakan privasi IoT dalam konteks *smart cities* [1], [2], [7], [16], [20], [25]. Pendekatan ini dipilih untuk memperoleh pemahaman yang komprehensif dan terstruktur mengenai bagaimana teknologi IoT diimplementasikan dalam lingkungan perkotaan cerdas, serta bagaimana aspek keamanan dan kebijakan privasi dibahas, diterapkan, dan dievaluasi dalam penelitian-penelitian terdahulu [4], [6]. Metode SLR digunakan karena mampu mensintesis temuan dari berbagai studi secara sistematis, transparan, dan dapat direplikasi, sehingga sesuai untuk mengidentifikasi pola, tantangan, serta kesenjangan penelitian terkait keamanan dan privasi IoT pada *smart cities* [2], [7], [11], [16], [20], [25]. Selain itu, pendekatan konseptual digunakan untuk mengintegrasikan hasil SLR ke dalam kerangka analisis yang menghubungkan dimensi teknis, kebijakan, dan tata kelola kota [8], [9]. Alur tahapan penelitian secara keseluruhan ditunjukkan pada Gambar 1, yang menggambarkan proses mulai dari identifikasi masalah hingga perumusan kerangka analisis keamanan dan kebijakan privasi IoT pada *smart cities*.



Gambar 1. Tahapan Penelitian Analisis Keamanan dan Kebijakan Privasi IoT pada *Smart Cities*

JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 4 No 3 February 2026
Hal: 2076-2086
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v4i3.802

2.2 *Literature Review*

Literature Review (LR) dalam penelitian ini disusun menggunakan pendekatan *Systematic Literature Review* (SLR) untuk mengidentifikasi, mengevaluasi, dan mensintesis penelitian-penelitian terdahulu yang membahas keamanan dan kebijakan privasi *Internet of Things* (IoT) dalam konteks *smart cities*. Proses ini bertujuan untuk memperoleh gambaran komprehensif mengenai tantangan teknis, aspek kebijakan, serta pendekatan tata kelola data yang telah dikaji dalam literatur ilmiah terkini.

Penelusuran literatur dilakukan pada basis data ilmiah bereputasi seperti Scopus, ScienceDirect, IEEE Xplore, SpringerLink, dan MDPI dengan rentang publikasi tahun 2022-2025. Berdasarkan kriteria inklusi dan eksklusi yang telah ditetapkan, diperoleh 25 artikel ilmiah terpilih yang relevan dengan fokus penelitian ini. Ringkasan karakteristik dan kontribusi utama dari literatur terpilih disajikan pada Tabel 1.

Analisis terhadap literatur menunjukkan bahwa penerapan IoT pada *smart cities* memberikan kontribusi signifikan terhadap efisiensi layanan publik, manajemen sumber daya, dan pengambilan keputusan berbasis data. Namun demikian, berbagai penelitian menegaskan bahwa sistem IoT juga menghadapi ancaman keamanan dan risiko privasi yang kompleks akibat heterogenitas perangkat, konektivitas terbuka, serta keterbatasan mekanisme keamanan end-to-end [1], [4], [16], [21], [24], [25].

Sejumlah studi menyoroti bahwa kebijakan privasi dan regulasi yang ada umumnya masih bersifat normatif dan belum sepenuhnya selaras dengan karakteristik data IoT yang bersifat *real-time*, terdistribusi, dan masif [9], [18], [19], [20]. Kondisi ini berpotensi menimbulkan kesenjangan antara perlindungan data secara hukum dan praktik teknis di lapangan, yang pada akhirnya dapat menurunkan kepercayaan publik terhadap layanan *smart city*.

Selain pendekatan kebijakan, beberapa penelitian mengusulkan integrasi teknologi pendukung seperti *blockchain, artificial intelligence, federated learning*, dan *digital twin* sebagai solusi untuk meningkatkan keamanan, transparansi, dan perlindungan privasi data dalam ekosistem *smart city* [6], [8], [14], [17]. Meskipun demikian, literatur juga menekankan bahwa solusi teknis saja tidak cukup tanpa didukung oleh tata kelola data dan kebijakan privasi yang adaptif dan terintegrasi [11], [18], [20].

Berdasarkan sintesis literatur yang dirangkum pada Tabel 1, dapat disimpulkan bahwa penelitian mengenai keamanan dan kebijakan privasi IoT pada *smart cities* masih menghadapi tantangan multidimensi. Oleh karena itu, diperlukan pendekatan integratif yang menggabungkan mekanisme keamanan teknis, kebijakan privasi yang jelas, serta tata kelola data yang akuntabel untuk mendukung pengembangan *smart cities* yang berkelanjutan dan berorientasi pada perlindungan data warga.

Tabel 1. Ringkasan *Literature Review* Keamanan dan Privasi IoT pada *Smart Cities*

Penulis (Tahun)	Fokus Penelitian	Metodologi	Kontribusi Utama
Javaid et al. (2025)	IoT pada *smart hospitals*	*Literature review*	IoT meningkatkan efisiensi layanan, namun keamanan & privasi krusial [1]
Kozar et al. (2025)	*Green IoT & smart city*	*Bibliometric review*	GIoT mendukung keberlanjutan, gap kebijakan masih ada [2]
Podder et al. (2024)	*IoT & HR analytics*	Kuantitatif	IoT berpengaruh signifikan, isu privasi data karyawan [3]
Aldehim et al. (2025)	*5G-oT smart city*	*Literature review*	Keamanan dan regulasi menentukan keberhasilan *smart city* [4]
Yessef et al. (2025)	*Digital twin smart city*	SLR	*Digital twin* efektif, bergantung pada keamanan data [5]
Al Barwani et al. (2023)	Keamanan IoT *smart city*	Review	*Blockchain* meningkatkan keamanan dan transparansi [6]
Santoso et al. (2024)	*Smart city* Indonesia	Bibliometric	Riset dominan teknis, kurang kebijakan & tata kelola [7]
Almulhim (2025)	IoT-blockchain	SLR (PRISMA)	Integrasi meningkatkan kepercayaan dan keamanan [8]
Ilhami (2022)	Privasi *smart city*	SLR	IoT & *blockchain* penting untuk proteksi data [9]
Fadjri et al. (2025)	Kebijakan privasi IoT	Survei	Literasi privasi pengguna masih rendah [10]
Wijaya et al. (2025)	IT *governance*	Mixed-method	Tata kelola TI menurunkan risiko pelanggaran data [11]
Putra et al. (2023)	IoT sehari-hari	Kualitatif	Risiko privasi meningkat tanpa kesadaran pengguna [12]
Anwar & Sanmorino	Regulasi IoT	Yuridis	Standar keamanan global diperlukan [13]

JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 4 No 3 February 2026
Hal: 2076-2086
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v4i3.802

Penulis (Tahun)	Fokus Penelitian	Metodologi	Kontribusi Utama
(2024)			
Ragab et al. (2025)	AI & *federated learning*	SLR	*Privacy-by-design* penting pada smart city [14]
Haider et al. (2025)	IoT & *real-time marketing*	Mixed-method	Perlindungan data krusial untuk kepercayaan pengguna [15]
Wakili & Bakkali (2025)	Keamanan IoT	SLR	Pendekatan hybrid paling efektif [16]
Dubey et al. (2025)	EV *smart city*	Simulasi	IOTA meningkatkan privasi dan skalabilitas [17]
Jin & Wang (2025)	Regulasi data *smart city*	Normatif	Kerangka regulasi terintegrasi dibutuhkan [18]
Lnenicka et al. (2024)	Big data & privasi	Content + Delphi	Perlindungan data belum merata [19]
Bhardwaj et al. (2024)	*Tren global IoT*	SLR	Keamanan & privasi isu utama masa depan [20]
Alotaibe (2024)	Model keamanan IoT	Metamodeling	Keamanan IoT lebih terintegrasi [21]
Mohammad et al. (2022)	Autentikasi IoT	Simulasi	Serangan IoT dapat diminimalkan [22]
Zheng (2022)	*Blockchain smart city*	Konseptual	Transparansi dan kontrol akses meningkat [23]
Rao & Deebak (2023)	Keamanan IoT	Survey	Autentikasi & *key management* krusial [24]
Ahmed & Chitra (2025)	Isu keamanan IoT	SLR	Pendekatan *end-to-end* diperlukan [25]

2.3 Objek dan Ruang Lingkup Penelitian

Objek penelitian ini adalah sistem *Internet of Things* (IoT) yang digunakan dalam implementasi *smart cities*, baik pada sektor layanan publik maupun infrastruktur perkotaan [1], [3]. Penelitian ini tidak berfokus pada satu kota atau studi kasus spesifik, melainkan pada ekosistem IoT *smart city* secara konseptual dan lintas konteks berdasarkan literatur ilmiah yang relevan [4], [7]. Literatur yang dianalisis dalam penelitian ini mencakup publikasi ilmiah pada rentang tahun 2022-2025, sejalan dengan perkembangan signifikan teknologi IoT, keamanan siber, dan kebijakan privasi dalam konteks *smart cities*.

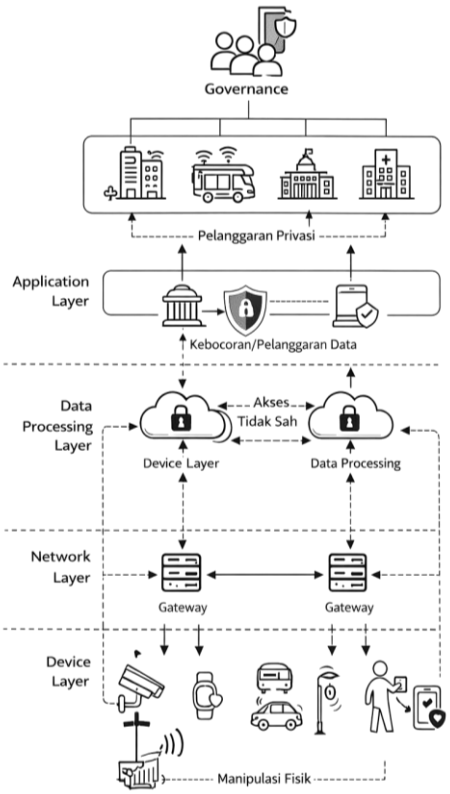
Ruang lingkup penelitian dibatasi pada tiga aspek utama. Pertama, keamanan IoT, yang mencakup ancaman, kerentanan, dan mekanisme perlindungan data pada sistem IoT *smart city* [6], [11]. Kedua, privasi data, yang berfokus pada perlindungan data warga, pengelolaan data sensitif, serta implikasi kebocoran dan penyalahgunaan data [9], [10], [12]. Ketiga, kebijakan dan regulasi, yang mencakup kebijakan privasi, tata kelola data, serta regulasi yang mengatur implementasi IoT dalam lingkungan *smart cities* [9], [13]. Pembatasan ruang lingkup ini dilakukan agar analisis tetap fokus dan mendalam sesuai dengan tujuan penelitian.

2.4 Arsitektur IoT dalam *Smart Cities* yang Dianalisis

Analisis dalam penelitian ini mengacu pada arsitektur IoT *smart city* yang bersifat berlapis (*layered architecture*), yang umumnya terdiri dari lapisan perangkat (*device layer*), lapisan jaringan (*network layer*), lapisan pengolahan data (*data processing layer*), dan lapisan aplikasi (*application layer*) [4], [5], [6], [16], [21], [24], [25]. Setiap lapisan memiliki peran dan karakteristik yang berbeda dalam pengelolaan data serta tingkat risiko keamanan dan privasi yang bervariasi.

Lapisan perangkat berfungsi sebagai pengumpul data melalui sensor dan aktuator, yang rentan terhadap manipulasi fisik dan akses tidak sah [6], [12]. Lapisan jaringan bertanggung jawab atas transmisi data dan menghadapi risiko penyadapan serta serangan komunikasi [4], [14]. Lapisan pengolahan data, yang umumnya berbasis *cloud* atau *edge computing*, berisiko terhadap kebocoran data dan pelanggaran privasi akibat pengelolaan data berskala besar [5], [14]. Sementara itu, lapisan aplikasi berinteraksi langsung dengan pengguna dan institusi, sehingga berkaitan erat dengan kebijakan privasi dan kepercayaan publik [9], [10]. Representasi arsitektur IoT *smart city* beserta titik-titik risiko keamanan dan privasi ditunjukkan pada Gambar 2.

JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 4 No 3 February 2026
Hal: 2076-2086
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v4i3.802



Gambar 2. Arsitektur IoT pada Smart Cities dan Titik Risiko Keamanan serta Privasi
Sumber : diadaptasi oleh penulis dari [4], [5], [6]

2.5 Teknik Analisis Keamanan IoT

Analisis keamanan IoT dalam penelitian ini dilakukan dengan pendekatan analisis konseptual berbasis prinsip *Confidentiality, Integrity, dan Availability* (CIA). Setiap lapisan arsitektur IoT dianalisis untuk mengidentifikasi potensi ancaman terhadap kerahasiaan data, integritas informasi, dan ketersediaan layanan [6], [11], [16], [21], [24], [25]

Selain itu, penelitian ini mengkaji teknik keamanan yang umum dibahas dalam literatur, seperti enkripsi data, autentikasi dan otorisasi pengguna, manajemen identitas perangkat, serta pemanfaatan teknologi pendukung seperti *blockchain* dan *artificial intelligence* dalam konteks *smart cities* [4], [6], [14]. Analisis ini tidak bertujuan untuk menguji implementasi teknis secara eksperimental, melainkan untuk mengevaluasi kecukupan dan keterbatasan pendekatan keamanan yang diusulkan dalam penelitian-penelitian sebelumnya. Hasil analisis keamanan IoT berdasarkan lapisan sistem dan jenis ancaman dirangkum dalam Tabel 2.

Tabel 2. Analisis Keamanan IoT pada *Smart Cities* Berdasarkan Lapisan Sistem [4], [6], [11], [14]

Lapisan Sistem IoT	Fungsi Utama	Ancaman Keamanan Utama	Risiko terhadap Data & Privasi	Pendekatan Keamanan yang Direkomendasikan
Device Layer	Mengumpulkan data melalui sensor dan aktuator (kamera, sensor lingkungan, wearable, kendaraan pintar)	Manipulasi fisik perangkat, pencurian perangkat, malware pada sensor	Kebocoran data mentah, pemalsuan data, pelanggaran privasi individu	Autentikasi perangkat, *secure boot*, enkripsi data di perangkat, perlindungan fisik
Network Layer	Mentransmisikan data dari perangkat ke sistem pusat melalui gateway dan jaringan komunikasi	Penyadapan komunikasi, *man-in-the-middle attack*, *denial of service (DoS)*	Intersepsi data sensitif, gangguan layanan publik	Enkripsi komunikasi, protokol jaringan aman, firewall, IDS/IPS
Data Processing Layer	Menyimpan dan memproses data IoT pada *cloud* atau *edge computing*	Akses tidak sah, kebocoran data, *data tampering*	Eksposur data berskala besar, pelanggaran privasi massal	Kontrol akses berbasis peran, enkripsi data tersimpan, audit keamanan

JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 4 No 3 February 2026
Hal: 2076-2086
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v4i3.802

Lapisan Sistem IoT	Fungsi Utama	Ancaman Keamanan Utama	Risiko terhadap Data & Privasi	Pendekatan Keamanan yang Direkomendasikan
Application Layer	Menyediakan layanan dan antarmuka bagi pengguna dan institusi	Penyalahgunaan hak akses, celah aplikasi, kesalahan konfigurasi	Penyalahgunaan data pengguna, pelanggaran kebijakan privasi	Manajemen identitas pengguna, *access control*, penerapan *privacy-by-design*
Governance Layer	Mengatur kebijakan, regulasi, dan tata kelola data IoT	Lemahnya regulasi, ketidaksesuaian kebijakan dengan praktik teknis	Rendahnya perlindungan hak privasi dan kepercayaan publik	Kebijakan privasi yang jelas, kepatuhan regulasi, tata kelola data terintegrasi

2.6 Analisis Kebijakan Privasi dan Regulasi yang Digunakan

Analisis kebijakan privasi dalam penelitian ini dilakukan dengan menelaah kebijakan privasi dan regulasi yang dibahas dalam literatur terkait IoT dan *smart cities* [9], [13]. Fokus analisis diarahkan pada bagaimana kebijakan tersebut mengatur pengumpulan, penggunaan, penyimpanan, dan distribusi data, serta sejauh mana kebijakan tersebut mampu melindungi privasi warga [10], [12].

Penelitian ini juga menganalisis kesesuaian antara kebijakan privasi dan praktik teknis IoT yang diterapkan dalam *smart cities*. Aspek yang dianalisis meliputi transparansi kebijakan, kejelasan hak pengguna, mekanisme persetujuan (*consent*), serta tanggung jawab pengelola data [9], [10]. Evaluasi kebijakan privasi dan regulasi yang sering digunakan dalam konteks *smart city* dirangkum dalam Tabel 3.

Tabel 3. Evaluasi Kebijakan Privasi dan Regulasi dalam Implementasi IoT *Smart Cities* [9], [10], [11], [13]

Aspek Kebijakan / Regulasi	Deskripsi	Kekuatan	Kelemahan / Tantangan	Implikasi terhadap *Smart Cities*
Perlindungan Data Pribadi	Pengaturan terkait pengumpulan, penggunaan, dan penyimpanan data pribadi warga	Memberikan dasar hukum perlindungan privasi	Implementasi belum merata; mekanisme pengawasan terbatas	Risiko kebocoran data dan pelanggaran privasi warga
Transparansi Kebijakan Privasi	Ketersediaan dan kejelasan informasi kebijakan privasi kepada pengguna	Meningkatkan kesadaran dan kepercayaan publik	Bahasa kebijakan kompleks dan sulit dipahami pengguna	Rendahnya pemahaman masyarakat terhadap pengelolaan data
Persetujuan Pengguna (*Consent*)	Mekanisme persetujuan pengguna atas pengumpulan dan pemrosesan data	Menjamin hak pengguna atas data pribadi	Persetujuan sering bersifat formalitas	Ketidakseimbangan antara kontrol pengguna dan pengelola sistem
Keamanan Data dan Sistem	Ketentuan keamanan teknis dan manajerial dalam pengelolaan data IoT	Mendukung perlindungan data dari ancaman siber	Standar keamanan tidak seragam	Kerentanan sistem IoT terhadap serangan siber
Akuntabilitas dan Tanggung Jawab	Penetapan tanggung jawab pengelola data dan penyedia layanan	Mendorong tata kelola data yang lebih baik	Penegakan hukum belum optimal	Menurunnya kepercayaan publik terhadap *smart city*
Kepatuhan terhadap Regulasi	Kepatuhan sistem IoT terhadap regulasi nasional dan internasional	Menyelaraskan praktik lokal dengan standar global	Tantangan harmonisasi regulasi lintas sektor	Kompleksitas implementasi *smart city* berbasis IoT

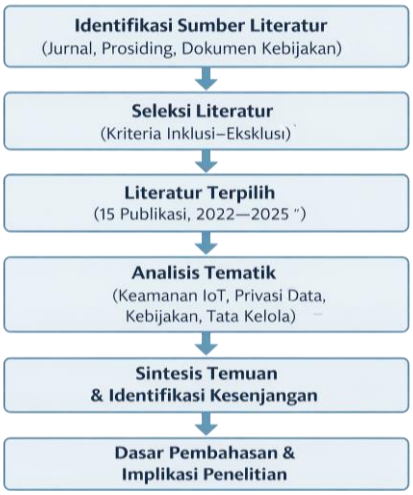
JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 4 No 3 February 2026
Hal: 2076-2086
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v4i3.802

Aspek Kebijakan / Regulasi	Deskripsi	Kekuatan	Kelemahan / Tantangan	Implikasi terhadap *Smart Cities*
Tata Kelola Data (*Data Governance*)	Pengaturan peran, proses, dan kontrol pengelolaan data	Mendukung pengelolaan data yang terstruktur	Belum terintegrasi dengan sistem teknis IoT	Fragmentasi pengelolaan data pada *smart cities*

2.7 Teknik Pengumpulan dan Analisis Data

Teknik pengumpulan data dalam penelitian ini dilakukan melalui studi literatur sistematis terhadap artikel jurnal, prosiding konferensi, dan dokumen kebijakan yang relevan [2], [7], [11]. Literatur diperoleh dari basis data ilmiah bereputasi dan diseleksi menggunakan kriteria inklusi dan eksklusi untuk memastikan relevansi dan kualitas sumber.

Data yang terkumpul dianalisis menggunakan analisis tematik, yaitu dengan mengelompokkan temuan literatur ke dalam tema-tema utama seperti ancaman keamanan IoT, risiko privasi data, kebijakan privasi, dan tata kelola *smart city* [4], [9], [14]. Selanjutnya, dilakukan sintesis temuan untuk mengidentifikasi pola, keterkaitan antar tema, serta kesenjangan penelitian. Hasil sintesis ini menjadi dasar dalam penyusunan pembahasan dan perumusan implikasi keamanan dan privasi terhadap pengembangan *smart cities* pada bagian selanjutnya [8], [15].



Gambar 3. Alur Teknik Pengumpulan dan Analisis Data Berbasis *Systematic Literature Review*

3. HASIL DAN PEMBAHASAN

3.1 Identifikasi Ancaman Keamanan pada Sistem IoT *Smart Cities*

Hasil analisis literatur menunjukkan bahwa sistem IoT pada *smart cities* menghadapi ancaman keamanan yang kompleks dan bersifat multidimensi [4], [6], [11], [14], [16], [21], [24], [25]. Ancaman tersebut muncul pada seluruh lapisan arsitektur IoT, mulai dari lapisan perangkat hingga lapisan aplikasi dan tata kelola [4], [5], [6], [21], [25]. Pada lapisan perangkat, ancaman utama meliputi manipulasi fisik sensor, pemasangan malware pada perangkat, serta pencurian perangkat IoT yang berpotensi menyebabkan kebocoran data mentah warga. Pada lapisan jaringan, ancaman yang dominan adalah penyadapan komunikasi, *man-in-the-middle attack,* dan *denial of service*, yang dapat mengganggu layanan publik berbasis IoT seperti transportasi dan manajemen lalu lintas [6], [12] , [16], [22], [24].

Lapisan pengolahan data dan aplikasi menghadapi ancaman berupa akses tidak sah, kebocoran data berskala besar, serta penyalahgunaan hak akses oleh pihak internal maupun eksternal [5], [11], [14]. Ancaman-ancaman ini menjadi semakin signifikan karena sistem *smart city* mengelola data dalam volume besar dan bersifat sensitif [1], [3]. Pemetaan ancaman keamanan IoT pada *smart cities* dirangkum dalam Tabel 4, yang menunjukkan hubungan antara jenis ancaman, lapisan sistem, dan dampak terhadap layanan kota.

Tabel 4. Pemetaan Ancaman Keamanan pada Sistem IoT *Smart Cities* [4], [6], [11], [12], [14], [16], [21], [24], [25]

Jenis Ancaman	Lapisan Sistem	Dampak Utama
Manipulasi perangkat	*Device Layer*	Kebocoran data, data palsu
Penyadapan jaringan	*Network Layer*	Intersepsi data sensitif
Akses tidak sah	*Data & Application Layer*	Pelanggaran privasi massal

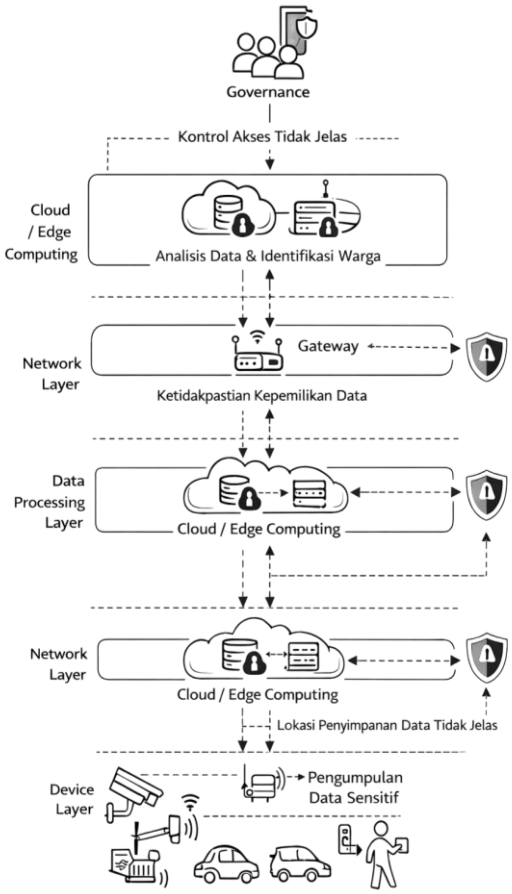
JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 4 No 3 February 2026
Hal: 2076-2086
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v4i3.802

Jenis Ancaman	Lapisan Sistem	Dampak Utama
Serangan DoS	*Network & Application Layer*	Gangguan layanan publik
Kelemahan tata kelola	*Governance Layer*	Rendahnya perlindungan data

3.2 Analisis Kerentanan Data dan Risiko Privasi

Analisis selanjutnya menunjukkan bahwa kerentanan data pada sistem IoT *smart cities* tidak hanya bersumber dari aspek teknis, tetapi juga dari cara data dikelola dan dimanfaatkan [9], [12], [14]. Data IoT umumnya dikumpulkan secara kontinu dan bersifat granular, sehingga memungkinkan dilakukan inferensi terhadap perilaku dan identitas individu [10], [12]. Risiko privasi muncul ketika data lokasi, pola mobilitas, atau data kesehatan warga dikombinasikan dan dianalisis tanpa kontrol yang memadai [1], [5], [9].

Kerentanan privasi juga diperkuat oleh penggunaan platform *cloud* dan *edge computing* yang sering kali melibatkan pihak ketiga [5], [14]. Ketidakjelasan mekanisme kepemilikan data, lokasi penyimpanan data, serta kontrol akses meningkatkan risiko penyalahgunaan data [9], [11]. Hubungan antara kerentanan data dan risiko privasi pada ekosistem IoT *smart cities* digambarkan secara konseptual pada Gambar 4, yang menunjukkan bagaimana aliran data lintas lapisan sistem berpotensi menimbulkan risiko privasi jika tidak diimbangi dengan mekanisme perlindungan yang memadai [4], [14].



Gambar 4. Alur Data IoT pada *Smart Cities* dan Titik Risiko Privasi
Sumber : dikembangkan oleh penulis berdasarkan [9], [12], [14], [18], [19]

3.3 Evaluasi Kebijakan Privasi dan Regulasi yang Berlaku

Evaluasi terhadap kebijakan privasi dan regulasi yang dibahas dalam literatur menunjukkan bahwa sebagian besar kebijakan telah menyediakan kerangka dasar perlindungan data pribadi [9], [13]. Namun, efektivitas kebijakan tersebut dalam konteks *smart cities* masih menghadapi berbagai tantangan [10], [11]. Kebijakan privasi sering kali disusun secara umum dan belum sepenuhnya mempertimbangkan karakteristik data IoT yang bersifat *real-time*, terdistribusi, dan lintas sektor [9], [14].

Selain itu, implementasi kebijakan privasi sering kali tidak sejalan dengan praktik teknis di lapangan [10], [12]. Misalnya, mekanisme persetujuan pengguna (*consent*) cenderung bersifat formalitas dan tidak memberikan kontrol yang nyata kepada warga terhadap data mereka [10]. Evaluasi komparatif antara kebijakan privasi dan praktik

JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 4 No 3 February 2026
Hal: 2076-2086
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v4i3.802

implementasi IoT *smart cities* disajikan dalam Tabel 5, yang menyoroti kesenjangan antara regulasi dan realitas teknis [9], [13].

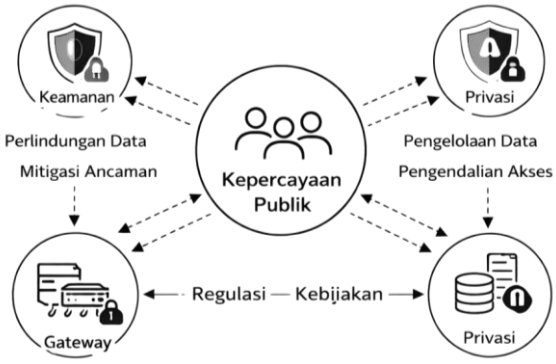
Tabel 5. Kesesuaian Kebijakan Privasi dan Praktik Implementasi IoT *Smart Cities* [9], [10], [11], [13], [18], [19]

Aspek	Kebijakan Privasi	Implementasi Teknis
Transparansi	Tersedia secara normatif	Sulit dipahami pengguna
Persetujuan pengguna	Diatur dalam kebijakan	Bersifat simbolis
Kontrol data	Dijanjikan	Terbatas pada pengelola
Penegakan	Diatur	Belum optimal

3.4 Dampak Keamanan dan Privasi terhadap Kepercayaan Publik

Keamanan dan privasi merupakan faktor kunci yang mempengaruhi kepercayaan publik terhadap implementasi *smart cities* [9], [11], [15]. Hasil sintesis literatur menunjukkan bahwa rendahnya tingkat keamanan dan perlindungan privasi berpotensi menurunkan kepercayaan warga, yang pada akhirnya dapat menghambat adopsi layanan *smart city* [10], [12]. Warga cenderung enggan menggunakan layanan berbasis IoT apabila merasa data pribadinya tidak aman atau berpotensi disalahgunakan [10], [15].

Hubungan antara keamanan, privasi, dan kepercayaan publik digambarkan pada Gambar 5, yang menunjukkan bahwa peningkatan keamanan teknis dan kebijakan privasi yang jelas dapat meningkatkan kepercayaan warga terhadap layanan *smart city* [9], [11].



Gambar 5. Hubungan Keamanan, Privasi, dan Kepercayaan Publik dalam *Smart Cities*
Sumber : disintesis oleh penulis berdasarkan [9], [11], [15], [19], [20]

3.5 Perbandingan dengan Penelitian Terkait

Dibandingkan dengan penelitian-penelitian terdahulu, hasil penelitian ini menunjukkan pendekatan yang lebih integratif [6], [8], [11]. Sebagian besar penelitian sebelumnya berfokus pada solusi teknis keamanan atau kajian kebijakan privasi secara terpisah [4], [6], [9]. Penelitian ini menggabungkan kedua perspektif tersebut dalam satu kerangka analisis yang mempertimbangkan aspek teknis, kebijakan, dan tata kelola *smart city* secara simultan [8], [11].

Perbandingan antara penelitian ini dan studi terkait disajikan dalam Tabel 6, yang menegaskan posisi dan kontribusi penelitian ini dalam literatur.

Tabel 6. Perbandingan Penelitian Ini dengan Penelitian Terkait

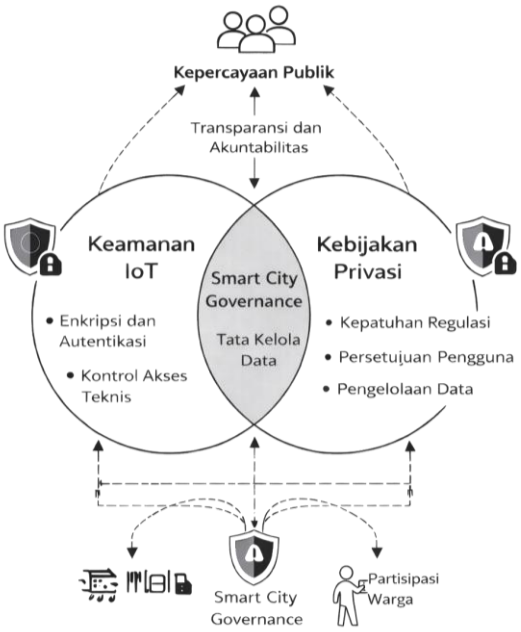
Aspek	Penelitian Terdahulu	Penelitian Ini
Fokus	Teknis atau kebijakan	Integratif
Perspektif	Parsial	Holistik
Konteks	Global / sektoral	*Smart city* kontekstual
Kontribusi	Konseptual	Kerangka analisis terpadu

3.5 Implikasi Keamanan dan Privasi terhadap Pengembangan *Smart Cities*

Implikasi dari hasil penelitian ini menunjukkan bahwa pengembangan *smart cities* harus menempatkan keamanan dan privasi sebagai komponen strategis, bukan sekadar pelengkap teknologi [4], [8], [11]. Keamanan IoT yang kuat tanpa kebijakan privasi yang efektif tidak akan mampu membangun kepercayaan publik, begitu pula sebaliknya [9], [15]. Oleh karena itu, diperlukan pendekatan terintegrasi yang menggabungkan mekanisme keamanan teknis, kebijakan privasi yang adaptif, serta tata kelola data yang transparan [8], [11], [14].

Implikasi konseptual dari pendekatan ini dirangkum dalam Gambar 6, yang menyajikan kerangka integratif keamanan dan kebijakan privasi IoT untuk pengembangan *smart cities* yang berkelanjutan.

JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 4 No 3 February 2026
Hal: 2076-2086
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v4i3.802



Gambar 6. Kerangka Integratif Keamanan IoT dan Kebijakan Privasi dalam Pengembangan *Smart Cities*
Sumber : dikembangkan oleh penulis berdasarkan [8], [11], [14], [16], [18], [20]

4. KESIMPULAN

Penelitian ini menganalisis keamanan dan kebijakan privasi dalam penggunaan teknologi *Internet of Things* (IoT) pada *smart cities* melalui pendekatan *Systematic Literature Review* (SLR) terhadap 25 publikasi ilmiah yang diterbitkan pada rentang tahun 2022-2025. Hasil kajian menunjukkan bahwa sistem IoT dalam lingkungan *smart cities* menghadapi ancaman keamanan dan risiko privasi yang kompleks dan multidimensi pada seluruh lapisan arsitektur sistem, mulai dari perangkat, jaringan, pengolahan data, hingga aplikasi dan tata kelola, yang tidak hanya dipengaruhi oleh kelemahan teknis tetapi juga oleh lemahnya integrasi antara mekanisme keamanan dan kebijakan privasi. Selain itu, kebijakan privasi yang ada umumnya masih bersifat normatif, kurang adaptif terhadap karakteristik data IoT yang *real-time* dan terdistribusi, serta belum sepenuhnya dipahami oleh pengguna, sehingga berpotensi menurunkan efektivitas perlindungan data dan kepercayaan publik. Temuan ini menegaskan bahwa pengembangan *smart cities* memerlukan pendekatan integratif yang memposisikan keamanan IoT, kebijakan privasi, dan tata kelola data yang transparan sebagai komponen strategis untuk mendukung keberlanjutan dan kepercayaan publik.

REFERENCES

[1] M. Javaid, A. Haleem, R. P. Singh, R. Suman, S. Khan, and S. Rab, "Adoption of Internet of Things for smart city-enabled smart hospitals," *Intell. Hosp.*, vol. 1, no. 2, p. 100011, Dec. 2025, doi: 10.1016/j.inhs.2025.100011.

[2] Ł. J. Kozar, A. Podgórniak-Krzykacz, and J. Przywojska, "The Role and Significance of the Green Internet of Things in Smart City Development: A Bibliometric Review of Research Trends," *Procedia Comput. Sci.*, vol. 270, pp. 4495–4504, 2025, doi: 10.1016/j.procs.2025.09.575.

[3] S. K. Podder, D. Samanta, and B. Prevalla Etemi, "Impact of Internet of Things (IoT) applications on HR analytics and sustainable business practices in smart city," *Meas. Sensors*, vol. 35, p. 101296, Oct. 2024, doi: 10.1016/j.measen.2024.101296.

[4] G. Aldehim *et al.*, "Balancing sustainability and security: A review of 5G and IoT in smart cities," *Digit. Commun. Networks*, vol. 11, no. 6, pp. 1722–1737, Dec. 2025, doi: 10.1016/j.dcan.2025.06.007.

[5] M. Yessef, Y. Hakam, M. Tabaa, M. M. Alammar, and Z. M. S. Elbarbary, "Digital twin technology in smart cities: A step toward intelligent urban management," *Energy Reports*, vol. 14, pp. 5539–5557, Dec. 2025, doi: 10.1016/j.egyr.2025.11.097.

[6] B. Al Barwani, E. Al Maani, and B. Kumar, "IoT-Enabled Smart Cities: A Review of Security Frameworks, Privacy, Risks and Key Technologies," in *Proceedings of the 1st International Conference on Innovation in Information Technology and Business (ICIITB 2022)*, Dordrecht: Atlantis Press International BV, 2023, pp. 83–95. doi: 10.2991/978-94-6463-110-4_8.

[7] A. D. Santoso, J. E. Aryansah, and A. Nasyaya, "Writing about smart cities in Indonesia: A bibliometric analysis," *J. Reg. City Plan.*, vol. 35, no. 1, pp. 69–89, Apr. 2024, doi: 10.5614/jpwk.2024.35.1.4.

JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 4 No 3 February 2026
Hal: 2076-2086
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v4i3.802

[8] A. I. Almulhim, "A Conceptual Framework for Integrating IoT and Blockchain for Smart and Sustainable Urban Development," *Smart Cities*, vol. 8, no. 6, p. 209, Dec. 2025, doi: 10.3390/smartcities8060209.
[9] D. A. S. Ilhami, "Data Privasi dan Keamanan Siber pada Smart-City: Tinjauan Literatur," *SNATI*, vol. 2, no. 1, pp. 51–60, 2022.
[10] M. A. Fadjri, A. R. A. AL, and R. Amalia, "Analisis Kebijakan Privasi pada Aplikasi Mobile IoT: Dampak Terhadap Keamanan Pengguna di Kalangan Mahasiswa," *Innov. Comput. Educ. J.*, vol. 1, no. 2, pp. 78–84, 2025.
[11] A. F. Wijaya, M. Lestari, and F. Angelica, "OPTIMIZING IT GOVERNANCE FOR ENHANCED SECURITY IN SMART CITIES," *JITK (Jurnal Ilmu Pengetah. dan Teknol. Komputer)*, vol. 11, no. 1, pp. 44–54, Aug. 2025, doi: 10.33480/jitk.v11i1.6639.
[12] F. P. E. Putra, S. M. Dewi, Maugfiroh, and A. Hamzah, "Jurnal Sistim Informasi dan Teknologi https://jsisfotek.org/index.php Privasi dan Keamanan Penerapan IoT Untuk Kehidupan Sehari-Hari : Tantangan dan Implikasi," vol. 5, no. 2, pp. 26–32, 2023, doi: 10.37034/jsisfotek.v5i1.232.
[13] Y. Z. Anwar and A. Sanmorino, "Hukum dan Kebijakan Keamanan Siber: Tantangan Regulasi Perangkat IoT," *J. Ilm. Inform. Glob.*, vol. 15, no. 3, pp. 95–99, Nov. 2024, doi: 10.36982/jiig.v15i3.4773.
[14] M. Ragab *et al.*, "Advanced artificial intelligence with federated learning framework for privacy-preserving cyberthreat detection in IoT-assisted sustainable smart cities," *Sci. Rep.*, vol. 15, no. 1, p. 4470, Feb. 2025, doi: 10.1038/s41598-025-88843-2.
[15] Raiyan Haider, Farhan Abrar Ibne Bari, Osru, Nishat Afia, and Mohammad Abiduzzaman khan Mugdho, "Leveraging internet of things data for real-time marketing: Opportunities, challenges, and strategic implications," *Int. J. Sci. Res. Arch.*, vol. 15, no. 3, pp. 1657–1663, 2025, doi: 10.30574/ijsra.2025.15.3.1936.
[16] A. Wakili and S. Bakkali, "Privacy-preserving security of IoT networks: A comparative analysis of methods and applications," *Cyber Secur. Appl.*, vol. 3, p. 100084, Dec. 2025, doi: 10.1016/j.csa.2025.100084.
[17] C. Dubey, A. K. Singh, and S. Sachan, "Governing smart city EV networks: A privacy-preserving, IOTA-based architecture for decentralized urban infrastructure," *Urban Gov.*, vol. 5, no. 4, pp. 512–526, Nov. 2025, doi: 10.1016/j.ugj.2025.10.001.
[18] Y. Jin and Y. Wang, "Reassessing smart city development and personal data protection: A regulatory framework," *Int. Rev. Econ. Financ.*, vol. 99, p. 104022, Apr. 2025, doi: 10.1016/j.iref.2025.104022.
[19] M. Lnenicka, P. Hervert, and O. Horak, "Understanding big data and data protection measures in smart city strategies: An analysis of 28 cities," *Urban Gov.*, vol. 4, no. 4, pp. 255–273, Nov. 2024, doi: 10.1016/j.ugj.2024.12.008.
[20] V. Bhardwaj, A. Anooja, L. S. Vermani, Sunita, and B. K. Dhaliwal, "Smart cities and the IoT: an in-depth analysis of global research trends and future directions," *Discov. Internet Things*, vol. 4, no. 1, p. 19, Oct. 2024, doi: 10.1007/s43926-024-00076-3.
[21] D. Z. Alotaibe, "IoT Security Model for Smart Cities based on a Metamodeling Approach," *Eng. Technol. Appl. Sci. Res.*, vol. 14, no. 3, pp. 14109–14118, Jun. 2024, doi: 10.48084/etasr.7132.
[22] A. Mohammad, H. Al-Refai, and A. Alawneh, "User Authentication and Authorization Framework in IoT Protocols," *Computers*, vol. 11, no. 10, p. 147, Sep. 2022, doi: 10.3390/computers11100147.
[23] W. Zheng, "A Blockchain-based Data Sharing Platform for Smart Cities," 2022. doi: 10.2991/978-94-6463-108-1_10.
[24] P. M. Rao and B. D. Deebak, "Security and privacy issues in smart cities/industries: technologies, applications, and challenges," *J. Ambient Intell. Humaniz. Comput.*, vol. 14, no. 8, pp. 10517–10553, Aug. 2023, doi: 10.1007/s12652-022-03707-1.
[25] S. Ahmed and C. K., "A Review of IoT Security Issues in Smart City Systems," *J. Innov. Technol.*, vol. 2025, no. 2, Dec. 2025, doi: 10.61453/joit.v2025no24.